Emergence of Fintech and cybersecurity in a global financial centre

Strategic approach by a regulator

Artie W. Ng and Benny K.B. Kwok
School of Professional Education and Executive Development, The Hong Kong Polytechnic University, Kowloon, Hong Kong

Abstract

Purpose – This paper aims to explore how the regulator of a global financial centre (GFC) under an international trend of adopting emerging technologies for financial services (Fintech) articulates such opportunities and risks strategically.

Design/methodology/approach – With a literature review on the global regulatory environment and the underlying risks related to Fintech, it looks into the formulation and implementation of complementary regulatory policies in the case of Hong Kong as a GFC. Relevant policy documents disclosed by the financial regulator on cybersecurity and pertinent issues are examined.

Findings – Adopting a strategic approach that seizes opportunities associated with Fintech, the financial regulator harnesses comprehensive risk-based mechanisms to embrace exposures to cyber risks while promoting institutionalization of cybersecurity among the regulated firms with strategic controls. This study suggests a pathway for the evolution of a profession with both technical and ethical competence for mitigating the emerging risks arising from Fintech. However, such an approach is yet to be tested with respect to efficacy for the unexplored territories of fraud exposures, resulting from swift Fintech developments across borders.

Research limitations/implications – As Fintech has only emerged rapidly in the recent years, it is not conclusive in this review of performance and effectiveness of the financial regulator in its strategic approach. Further studies may utilize a longitudinal method to analyze and examine the regulatory measures undertaken by financial regulators in various GFCs.

Originality/value – This study reveals a strategic approach adopted by an emerged GFC in embracing Fintech innovation that however brings about unidentified risks and potential frauds to its financial services sector. Pertinent anti-fraud and cybersecurity measures are highlighted.

Keywords Hong Kong, Fraud, Cybersecurity, Fintech, Global financial centre, Risk-based approach

Paper type General review

1. Introduction

Subsequent to the financial crisis in 2008, global financial centres (GFCs) and financial institutions have looked into new business development opportunities to sustain their industry, as increased regulatory measures escalate the cost of operations. One of their recent initiatives is to adopt emerging information and internet technologies to enhance the delivery of their financial services (Fintech). There are high hopes that Fintech, particularly Blockchain as a solution for secure information technology and data security, will bring along development of innovative financial products and services as well as potential improvement in efficiency of operations in the financial services industry (Guo and Liang, 2016; Zhu and Zhou, 2016). The financial regulators around the world tempt to embrace such an

Journal of Financial Regulation and Compliance
Vol. 25 No. 4, 2017
pp. 422-434

1358-1988
DOI 10.1108/JFRC-01-2017-0013

opportunity while developing regulatory measures to enable the development of Fintech as a global trend. Such an approach by a regulatory body is considered strategic for sustaining a GFC. For instance, development of prudent regulations for Fintech has become imminent for Hong Kong to sustain itself as the GFC of China. As China continues its route to globalization, Chinese emerging multinational financial institutions are poised to utilize the platform of Hong Kong as a GFC to execute cross-border transactions, and thus are driven to comply with its financial regulations and related international practices.

In the past two decades, Hong Kong has emerged from its status as a British Colony and an international centre supporting regional trades in Asia to a GFC that endures relatively free flows of information and capital. Hong Kong has now positioned as a GFC predominantly for China by leveraging its Special Administrative Region legitimacy. Its stock market is recognized as one of the major stock exchanges in the world, in terms of market turnover and amounts of capital raised through initial public offering. Since the implementation of China's open-door policy in the early 1980s, Hong Kong has been providing a range of financial services for China's state-owned enterprises and entrepreneurial firms to facilitate financial capital raising as well as cross-border mergers and acquisitions.

Riding out the Asian and global financial crises in 1997 and 2008, Hong Kong strategically plans to augment its competitiveness as a GFC in Asia, comparable to its counterparts in London and New York. To support such a strategic imperative, the Hong Kong established its Financial Services Development Council (FSDC) in 2013. As reported by FSDC (2013):

> FSDC advises the Government on areas related to diversifying the financial services industry, enhancing Hong Kong's position and functions as an international financial centre of our country and in the region, and further consolidating our competitiveness through leveraging the Mainland to become more global.

FSDC (2013) also places emphasis on the importance of striking a balance between market development and financial stability, sustaining Hong Kong's international competitiveness without jeopardizing its financial regulatory standard.

Similar to other GFCs, Hong Kong opts to embrace innovation in financial services for potential business opportunities, despite the associated risks. In response to these regulatory measures, Hong Kong Monetary Authority (HKMA), as a paramount financial regulator of the banking sector, is seen adopting a risk-based approach, as endorsed internationally, in its policy formulation for dealing with the emergence of Fintech. As emerging technologies enable voluminous exchange of financial information and expedites the pace of global financial transactions, there are implications for a GFC to embrace Fintech so as to strengthen its strategic positioning with adequate regulations (Nicoletti, 2017). Studying the case of Hong Kong in light of such unexplored territories of Fintech, the authors argue that a new profession of cybersecurity must be developed, with competence in internal audit, management controls, risk management and information technology, to deal with the emergence of cyber risks in a GFC.

The following section provides a literature review addressing post-global financial crisis development, the initiatives on technological innovation for financial services as Fintech, its categorizations, potential frauds derived from Fintech and the growing importance of cybersecurity. The case of Hong Kong and its HKMA is reviewed by analysing its concerted range of regulatory measures in the recent years. The concluding remarks are provided to highlight the salient points in considering the way forward of regulating Fintech.

2. Post-financial crisis risk management and opportunity seeking

Instigated by the global financial crisis of 2008, financial regulators are among stakeholders concerned about the efficacy of existing regulatory architecture and measures (Martin, 2008). Risk management has been considered as a professional tool for dealing effectively with financial crises, subsequently adopted as a mechanism incorporated into the formal institutional response. Financial regulators have imposed more risk-management mechanisms, internal controls and compliance requirements (Prorokowski and Prorokowski, 2014; Ng and Tang, 2016). However, risk management-related mechanisms and the system in place would result in higher costs in banking operations. Economy of scale and scope of financial services offered have both become critical for financial institutions in search of sustainable profitability. Financial institutions also quest for sources of new revenue streams.

In addition to the role of rising capital, a GFC is increasingly seen as a place for effective wealth and asset management. Although one of the main focuses in the post-crisis development is the strengthening of financial regulatory measures, a GFC needs to look into financial services opportunities for its host financial institutions to survive (FSDC, 2013). GFCs would need to review legitimate opportunities that enable generating new revenues through product and service innovations while lowering their operating costs.

In the meantime, the rise of regional and global financial institutions in developing countries, beyond the pan-European and US multinational financial institutions, has further altered the regulatory landscape (Dy, 2016). In fact, four of the top ten international banks, ranked globally in terms of total assets, are state-owned banks from China[1]. A related major development noted by Dy (2016) is that RMB, the official currency of China, has become increasingly international through the issuing of offshore bonds outside the jurisdiction of origin, facilitated through China's global financial centre, Hong Kong. As globalization proceeds with mounting cross-border transactions, regulatory measures have not inhibited the flows of capital from one jurisdiction to another.

Despite continuous exploration of a global supervisory and regulatory framework, there are still many discrepancies in terms of policy, guidelines and enforcement among jurisdictions (Alexander *et al.*, 2006). Disruptive technologies newly introduced for applications could only compound the existing risks, creating an environment that is difficult for an individual, a local regulator to apprehend. Responsive regulatory measures should be anticipated for unidentified risks that would evolve with initiatives for innovation in financial services (Ng and Tang, 2016). Hong Kong positioned as a GFC of China is poised to retain its competitiveness against its rivals, such as Singapore and Shanghai, in the region through a strategic approach for Fintech adoption.

3. Emergence of Fintech innovation

Advances in computing technologies not only create opportunities to improve efficiency but also present challenges in the way the business of banking and financial services is performed. The traditional paper-based banking and financial services of the past are largely replaced by data digitalization in a networked environment. Technology-based firms attempt to enter into various areas of financial services through introduction of Fintech. Reportedly, more than 4,000 Fintech companies operate in the USA and the UK, while investment in Fintech companies since 2010 has been valued at more than $24bn globally (Arner *et al.*, 2015; Dy, 2016). However, regulation of Fintech still lacks a standard and is considered challenging due to data complications and newness of the knowledge involved (Treleaven, 2015).

3.1 Seeking innovation through Fintech

By enabling finance services through information technology, Fintech provides potential applications in two main areas. First, traditional financial institutions introduce new technologies into their e-banking operations with incorporation of innovative solutions for customers (Ernst & Young Global Ltd, 2015). For instance, enabling real-time drilling into a vast amount of data containing customers' demographic and psychographic profiles and spending patterns can support automated investment advice. Second, new or established technological companies that bring in new solutions or business models can "disrupt" the regulated financial services market – e.g. credit card issuers disrupted by e-wallets or smart-cards (PwC, 2016; Accenture, 2015).

In fact, the first reference to the term *Fintech* can be traced back to the early 1990s when it was introduced under the Financial Services Technology Consortium started by Citicorp (Hochsein, 2015). A recent survey by Accenture indicates that global investments in Fintech businesses grew by 75 per cent to $22.3bn in 2015, whereas those in Asia-Pacific increased four times to $4.3bn in 2015 (Accenture, 2016). New Fintech businesses can be further categorized into four specific solutions or ventures as summarized are as follows:

(1) *Efficient payment process*: By offering superior solutions for payment processing (such as banks and credit cards), Fintech facilitates faster payments across borders by mobile devices, e-wallets, digital currencies or other means, even at lower transaction costs (Bottomline Technologies, 2016; Avergun and Kukowski, 2016).

(2) *Robo-adviser*: Utilizing big data that overpowers human mental capacity and even the traditional computer databases, Fintech applies artificial intelligence (AI) and data-mining tools to create robo-advisers, with respect to investment advice and fund management. By removing inherent bias of human decision making, robo-advisers seek to capture all possible data and relevant trends, forming objective decisions and diversified spreads in portfolios (Allen and Overy, 2016).

(3) *Peer-to-peer (P2P) loan and deposit platform*: Fintech operates their lending and funding activities via a P2P platform (Avergun and Kukowski, 2016). Many of them utilize decentralized communication among peer users through a network, without passing through a central server (Kwok, 2016). Skipping the exchange or any intermediaries reduces transaction costs, resulting in savings to borrowers and depositors.

(4) *Crowdfunding*: These Fintech applications produce an online platform for various projects and business ventures to raise funds from a large number of donors or investors (Allen and Overy, 2016; Taylor Wessing, 2016). Crowdfunding is popular for companies at their early stage in the market, for securing donors or investors, along with engagement of new customers (who could be the same group of people). Another advantage claimed is that crowdfunding would facilitate formation of investment syndication, allowing for less experienced investors to rely on those with more experience.

3.2 Potential problems in Fintech

3.2.1 Potential frauds. Despite the business opportunities associated with Fintech, one could underestimate the frauds derived from a variety of emerging Fintech solutions. Such exposures could make business operations under digitalization vulnerable as there have not been many concerted international regulatory measures for Fintech (Treleaven, 2015). Fraud is a broad legal concept and involves the use of deception to obtain unfair and unlawful

gains (Kwok, 2005). Frauds cause direct and indirect losses and could expose the victims to civil or criminal liabilities – e.g. an employer may have to be held vicariously liable for its employees' wrongdoings. Identity theft, Ponzi schemes, phishing schemes and advanced-fee frauds are a few of the ways to defraud individuals (ACFE, 2016). Frauds against companies can be committed either internally by employees, directors or owners of companies; or externally by customers or vendors. Fraudsters defrauding Fintech may rely more on technology in the commission and concealment of various frauds, but the basics of frauds remain largely unchanged.

The "Fraud Triangle", as explored by Cressey (1973), is a model for explaining the three factors leading to fraudulent behaviours, which are:

- *pressure* under which fraudsters are driven by their need for money or other motives;
- *opportunity* that fosters the situation enabling frauds to occur and to be concealed; and
- *rationalization* with reference to the fraudsters' mindset in justifying to themselves committing frauds.

As the nature of frauds is largely similar across all kinds of businesses, these three factors are considered applicable to potential cases of fraud in Fintech. The term *Fraud Risk Factors* refers to events or conditions that indicate an incentive or pressure to commit fraud, or provide an opportunity to commit fraud (ISA, 2009). In general, Fraud Risk Factors in Fintech may fall into the following categories:

3.2.2 Excessive pressure to meet targets. Being in an emerging sector, only those Fintech applications with a clear competitive edge would survive in the marketplace. Fintech startups could be under excessive pressure to meet the targets or expectations of the market and stakeholders (Cressey, 1973), such as meeting revenue and profit projections imposed by directors, shareholders or parent companies. These startups could have difficulty in maintaining adequate working capital for research and development expenditures to stay competitive as well as managing liquidity to serve debt repayments and maintain other debt-covenant requirements. In addition, it is not unusual that many of these startups could only marginally pass or even fail to meet the listing requirements for taking their businesses to a new ground.

3.2.3 Untried business models and exposures to frauds. Many Fintech ventures operate on new business models of combining finance and technology, which often open up the vulnerability of their processes and internal controls. Fraudsters could perceive such weaknesses in such untried business models related to five main factors as explained in Table I.

3.3 Antifraud measures and cybersecurity for Fintech

In response to such potential frauds in Fintech, a series of cybersecurity initiatives is considered critical to preventing and mitigating such emerging risks in an IT-driven operation and environment. First, antifraud measures refer to tools, procedures or techniques to break one or more of the three factors in the "fraud triangle". Having proper internal controls in place is often an effective measure to remove the "opportunity" factor. Although the basics of fraud remain the same, fraudsters use new tools and techniques – particularly those driven by information technology – against Fintech (Deloitte LLP, 2015; Entrust, 2015). In response to such threats, any deterrence and detection measures should be adjusted accordingly. The characteristics of some Fintech solutions in contrast to other

Factors	Exposures to frauds
Regulatory uncertainties	Fintech ventures need to evaluate their businesses against accepted practices and applicable rules, regulations and legislation across all areas and borders on which they operate or base their activities (Allen and Overy, 2016). In other words, Fintech ventures have to evaluate whether their innovative products or services require licenses or approvals from the relevant authorities. Still, regulatory uncertainties remain high, posing a perceived opportunity for frauds
Excessive compliance costs	In addition to regulatory uncertainties, excessively high compliance costs may pressure many Fintech ventures to withdraw from the market. Costly analyses are required to assess whether innovative products fall within the regulatory regimes (Allen and Overy, 2016). When Fintech ventures expand globally as expected, expanding the business to different regulatory regimes could push compliance costs even higher. That is why "Fintech Bridges" was formed by the UK government, as an initiative to mitigate such problems (Baldwin, 2016). Fraudsters may perceive an opportunity for frauds, particularly when some Fintech ventures may not be in compliance due to cost concerns
Big data overpowering the human brain	The flood of a massive volume of structured or unstructured data can make the human brain and traditional databases, software and systems incapable in processing those data (Wolters Kluwer Financial Services, 2016), because of the volume of data, excessively fast speed of the data flows and data-processing capacity. Big data is seemingly eliminating human sense in distinguishing genuine entries and transactions from frauds
Lack of technological skills for the internal controls	In view of rapidly developing technology and innovation in Fintech, staff and systems involved in traditional internal controls or internal audits may not be equipped with the necessary skills to prevent and detect frauds in Fintech (Kellton Tech, 2016). Employees with the relevant knowledge and skills are likely to be in high demand. High turnover rates of staff are inevitable, and, together with inadequate management understanding of information technology, makes Fintech more vulnerable to frauds. Moreover, as brand new companies or new operations within existing businesses, Fintech ventures may not have the necessary policies and procedures for preventing and deterring their employees or vendors from committing fraud. Even if such policies and procedures exist, senior employees, placed with a high level of trust and responsibility, may abuse their authority. Also, pre-employment vetting may not have been properly conducted before bringing a senior employee on board
Loss of visible audit trail	Transactions and entries arranged through Fintech may not contain the same visible audit trails as those on a paper-based system (Garcia *et al.*, 2010; Manning, 2011). Without such step-by-step records by which the stated amounts are traced to their sources, a perceived opportunity for fraud may exist

Table I.
Factors in untried business models and exposures to frauds

traditional businesses are often related to anonymity, namely, the level and ambiguity of identity in the virtual world often give fraudsters the ease to conceal the source of hacking or wrongdoing (Avergun and Kukowski, 2016). Another issue with adopting Fintech is however related to the speed of processing transactions, payments and instructions at lightning speed that often suppresses the alert flag (Miller, 2015; Avergun and Kukowski, 2016).

Traditional or manual internal controls may not be able to keep up with the virtual world of Fintech (ACL Services, 2014). Besides, identity authentication is one of the main measures against hacking and anonymity problems in Fintech. Therefore, a range of so-called *RegTechs* to regulate potential frauds in Fintech has been proposed. Authentication tools, such as digital certificates, mobile device certificates and biometrics identification, can

provide a higher degree of security than traditional password logins (Rowntree, 2016). With respect to the main antifraud measures against the lightning speed of processing in Fintech, the following IT-based tools and software could be the essential safeguards. There are various analytics to evaluate data behaviours and users' activities (Li and Harris, 2016; Hein and Read, 2016; ACL Services, 2014; Bottomline Technologies, 2015). Common techniques, such as evaluating patterns of links and monitoring screens and keystroke hits, concerning suspicious items or activities under Detection by Common Techniques are highlighted as follows:

- missing, invalid, duplicated or out-of-sequence documents, reference numbers and control totals;
- deposits, withdrawals and other offsetting entries on the same account or IP address;
- enquiries or logins at out-of-ordinary times, dates or IP locations;
- deviations in statistical significance (i.e., those exceeding extreme highs or lows or fluctuating values exceeding the usual ranges and patterns); and
- data from different diverse sources bearing similar or even matching values (such as names, addresses, demographic details and account numbers) where such similarities should not exist.

Other specialized detecting techniques include:

- real-time alerts to identify anomalies with timely responses so as to avoid any losses of data and assets;
- examination of log files and real-time examining of network traffic and customer interface; and
- using investigative tools to rebuild links, screens and keystrokes in users' activities.

These safeguards should be adaptable to Fintech of all sizes, and the management or controllers should be able to adjust the thresholds and parameters to cater to their own needs. In addition to the above IT tools and software safeguards, some traditional internal control measures, based on the COSO framework, can prevent and detect frauds in operations (Fernández-Laviada, 2007; IRM, 2002; McNally, 2013). Basel Committee has also adopted a COSO-based assessment approach to assess operational risks of financial institutions (Mestchian *et al.*, 2005). Such measures promote top management's integrity and commitments to risk governance, prudent internal control processes and mitigating measures. Accordingly, the COSO framework facilitates a range of measures based on a risk-based approach composed of risk monitoring, assessment and responses. It emphasizes the functions of supervision and approval throughout the organization hierarchy as well as identifying certain unusual transactions and entries made by customers. More importantly, it suggests adopting a risk-based sampling technique for data analysis because frauds do not tend to occur randomly.

The concept and potential applications of COSO for internal control have in fact been widely adopted by accounting and financial professionals on a global basis (Ng and Mitchell, 2009; Ng and Ho, 2014). Its further applications as a comprehensive framework for assessing cyber risk, deterring frauds and enhancing cybersecurity in the financial industry are anticipated (Galligan and Rau, 2015). However, operational risk faced by banks could be further complicated with the emergence of Fintech in the banking sector. As reviewed by the Basel Committee, it is envisaged that self-assessment using scenario-based analyses would

be adopted in lieu of the COSO approach alone, so as to provide more insights about operational risks for the management (Kaiser, 2016).

4. The strategic approach of Hong Kong

4.1 Strengthening E-banking controls and advocating cybersecurity

Hong Kong, strategically positioned as the GFC of China, has the functions of raising capital in equity and debt, asset management for corporations and high net-worth individuals, as well as facilitating cross-border transactions. It has also been a well-sought-after regional and even global headquarters for multinationals in the financial services sector, such as HSBC and AIA. The city has proactively taken steps to strengthen its infrastructure while embracing market innovation with Fintech. In 2015, HKMA issued the *Supervisory Policy Manual on Risk Management of E-banking* to its regulated financial institutions, its guidelines on e-banking operations[2]. The policy manual has adopted a risk-based approach, comparable to the COSO framework, to ensure that the regulated banks follow through with prudent procedures, given the increased cyber risks in a global environment. HKMA subsequently issued a directive to all authorized institutions providing internet banking services to further strengthen their security controls, with regard for recent incidents involving unauthorized trading transactions[3].

In 2016, the Cybersecurity Fortification Initiative (CFI) was pursued by HKMA, to tighten its supervisory expectations for the regulated financial institutions' cybersecurity, focusing on three main initiatives, including the Cyber Resilience Assessment Framework, Professional Development Program and Cyber Intelligence Sharing Platform[4]. First, Cyber Resilience Assessment Framework adopts a risk-based framework for regulated financial institutions to assess their own risk profiles, with assessment on the level of defence and resilience, as well as appropriate protection against cyberattacks. Second, the Professional Development Program seeks to develop qualified professionals in cybersecurity. Third, cyber Intelligence Sharing Platform provides an effective infrastructure and platform for sharing intelligence on cyber attacks.

4.2 Embracing Fintech innovation

In the same year (2016), HKMA announced the establishment of the Fintech Innovation Hub to support research and adoption of Fintech by the industry[5]. It aims to be a neutral ground of the Fintech industry, where various stakeholders can collaborate to innovate. Industry players, such as banks, payment service providers and even new ventures, can collaborate to develop innovative ideas and evaluate new Fintech solutions.

As explained by the chief executive of HKMA, "Indiscriminate introduction of regulations might hinder the development of local financial technology solutions and a balance between market development and user protection is required" (Hong Kong Lawyer, 2016). Moreover, HKMA's "Fintech solutions" could bring benefits to the financial system while considering the "characteristics, potentials, and risks of Fintech". In doing so, HKMA decided to establish its Fintech Facilitation Office, with a mission to support the financial industry in facilitating the development of Fintech in Hong Kong, with three main functions, namely:

(1) working with the industry to promote research in Fintech solutions;

(2) providing a platform for industry communication and outreach activities; and

(3) acting as an interface and point of contact between Fintech market participants and regulators.

Accordingly, this initiative aims to be an effort of the financial regulator to sustain a GFC in the region, adopting a risk-based and technology-neutral approach in its financial supervision:

> This will help ensure the creation of an environment that is conducive to innovation and fair competition for market participants, while end users will not have to bear unnecessary or undue risk. (Hong Kong Lawyer, 2016).

Subsequently, HKMA launched its Fintech Supervisory Sandbox to nurture other innovative technologies for Fintech – namely, augmented reality, biometric authentication, Blockchain, robotics and mobile payment services[6]. This initiative would provide a supervisory arrangement with greater flexibility, to enable regulated banks to conduct more timely live tests of these initiatives in a secure environment, before a formal launch for banking and payment services. The three main initiatives of the HKMA strategic approach to countering cyber risks, and resultant human capital development, are articulated in Table II.

5. Concluding remarks

Striving to sustain Hong Kong's competiveness as the GFC of China, HKMA, the key financial regulator in Hong Kong, has responded with timely formulation and implementation of its strategic approach for embracing Fintech innovation. It has at the same time taken measures to tighten the regulatory system with cybersecurity and adoption of internationally accepted risk-management standards. This concerted approach remains to be tested for the increasingly high-volume, rapid, cross-border activities engineered by extensive use of internet technologies in wired, networked operations. Containment of risk by the financial regulators under such a global environment would become inevitably more challenging in a technologically accelerated pace with introduction of disruptive technologies, if not fully apprehended.

Institutionalization of a risk-based approach among the regulated is expected to provide a layer of precautionary measures in dealing with any unforeseeable situations resulting from the Fintech movement within a GFC that allows relatively free flow of information and capital. The initiatives to provide training and development to the existing staff in the financial services industry and to the next generation of cybersecurity talents would be a complementary measure in securing a pathway for

Table II.
Strategic approach by HKMA in countering cyber risks

Scope	Initiatives taken	Risk management and compliance measures	Human capital development
Enhancing existing banking operations	Safeguarding e-banking and internet banking operations	Directives for operational enhancements of regulated financial institutions	Upgrading knowledge about embracing cyber risk
Safeguarding integrity of GFC	Systemic risk governance and management with CFI	Comprehensive cybersecurity approach	Development of future risk-management professionals for the industry
Market innovation	Establishing Fintech Innovation Hub	Establishing Fintech Supervisory Sandbox	Preventive measures through early engagement of talents in the industry, universities and the science park

mitigating the ongoing concerns about the risks of e-banking operations while embracing the emerging Fintech industry.

Nevertheless, it is unlikely that such a strategic approach being implemented under a cyber environment would eliminate the potential frauds instigated by human beings in various scenarios. A baldly homogeneous risk-based approach as adopted would hardly detect various combinations of fraudulent activities and tactics deployed in cybercrimes related to financial services that could be potentially interconnected with money laundering activities. Integrity and ethical issues with Fintech would continue to remain salient at governance, management and individual levels. It is important to note that training and development for cybersecurity would not be effective without addressing the risks in fraud associated with human ethics and integrity (Brooks and Dunn, 2015, p. 496). Such ethical behaviour is even more critical for the Fintech professionals engaged in the overall design and development of the Fintech infrastructure.

Notes

1. This is based on the ranking provided by Forbes 2016.
2. Available at: www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf (accessed 19 January 2017).
3. Available at: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160526e1.pdf (accessed 19 January 2017).
4. Available at: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160524e1.pdf (accessed 26 January 2017).
5. Available at: www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/20160906e1-svf.pdf (accessed 26 January 2017).
6. Available at: www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160906e1.pdf (accessed 26 January 2017).

References

Accenture (2015), "The Future of Fintech and Banking: digitally disrupted or reimaged?", available at: www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf (accessed 21 November 2016).

Accenture (2016), "Fintech and the evolving landscape: landing points for the industry", available at: www.Fintechinnovationlabapac.com/media/1157/Fintech_Evolving_Landscape_2016.pdf (accessed 21 November 2016).

ACL Services (2014), "Fraud detection using data analytics in the banking industry", available at: www.acl.com/pdfs/DP_Fraud_detection_BANKING.pdf (accessed 3 December 2016).

Alexander, K., Dhumale, R. and Eatwell, J. (2006), *Global Governance of Financial System: The International Regulation of Systemic Risk*, Oxford University Press, New York, NY.

Allen and Overy (2016), "Fintech", available at: www.allenovery.com/SiteCollectionDocuments/Fintech.PDF (accessed 21 November 2016).

Arner, D.W., Barberis, J.N. and Buckley, R.P. (2015), "The Evolution of Fintech: A New Post-Crisis Paradigm?", University of Hong Kong Faculty of Law Research Paper No. 2015/047; UNSW Law Research Paper No. 2016-62, available at SSRN: http://ssrn.com/abstract=2676553 (assessed 30 November 2016).

Association of Certified Fraud Examiners (ACFE) (2016), "What is fraud?", available at: www.acfe.com/fraud-101.aspx (accessed 3 December 2016).

Avergun, J. and Kukowski, C. (2016), "Complying with AML Laws: challenges for the Fintech Industry", available at: www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-Fintech-industry/ (accessed 21 November 2016).

Baldwin, H. (2016), "First ever Fintech bridge established between Britain and Singapore", available at: www.gov.uk/government/news/first-ever-Fintech-bridge-established-between-britain-and-singapore (accessed 21 November 2016).

Bottomline Technologies (2015), "Insider Fraud", available at: www.bottomline.com/sites/default/files/cyber-fraud-insider-fraud-cfr-nae-ds-1505-012.pdf (accessed 3 December 2016).

Bottomline Technologies (2016), "Five Best Practices for Managing Global Payments in a Changing World", available at: http://archive.bottomline.com/collateral/payments/BT%20Five%20Best%20Practices%20for%20Managing%20Global%20Payments_WP_Web.pdf (accessed 21 November 2016).

Brooks, L.J. and Dunn, P. (2015), *Business and Professional Ethics*, Cengage Learning.

Cressey, D.R. (1973), *Other People's Money*, Patterson Smith, Montclair, NJ.

Deloitte LLP (2015), "2016 Hot topics for IT internal audit in financial services", available at: www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-audit-on-the-horizon.pdf (accessed 3 December 2016).

Dy, M. (2016), "The challenges to cross-border financial regulation in the post-financial crisis era", Centre for Banking and Finance Law, Faculty of Law, National University of Singapore, Report number CBFL-Rep-MD1, available at: http://law.nus.edu.sg/cbfl/pub_reports.htm (accessed 30 November 2016).

Entrust (2015), "3 ways financial institutions can improve fraud detection", available at: www.entrust.com/3-ways-financial-institutions-can-improve-fraud-detection/ (accessed 3 December 2016).

Ernst and Young Global Ltd (2015), "Fintech: are banks responding appropriately?", available at: www.ey.com/Publication/vwLUAssets/EY-Fintech-are-banks-responding-appropriately/$FILE/EY-Fintech-are-banks-responding-appropriately.pdf (accessed 21 November 2016).

Fernández-Laviada, A. (2007), "Internal audit function role in operational risk management", *Journal of Financial Regulation and Compliance*, Vol. 15 No. 2, pp. 143-155.

Financial Services Development Council (FSDC) (2013), "Strengthening Hong Kong as a Leading Global International Financial Centre", *Research Paper* No. 1, pp. 1-47.

Galligan, M.E. and Rau, K. (2015), "COSO in the cyber age", Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Garcia, R. May, C. and Zimbelman, M.F. (2010), "Not Just a Paper Trail", available at: www.fraud-magazine.com/article.aspx?id=2147483733 (accessed 21 November 2016).

Guo, Y. and Liang, C. (2016), "Blockchain application and outlook in the banking industry", *Financial Innovation*, Vol. 2 No. 1, p. 24.

Hein, H. and and Read, T. (2016), "The Problem with Financial Fraud Detection (and How to Improve It)", available at: http://haystax.com/technologyblog/2016/08/01/problem-financial-fraud-detection-improve/ (accessed 25 October 2016).

Hochsein, M. (2015), "Fintech (the Word, That Is) Evolves", American Banker, available at: www.americanbanker.com/bankthink/Fintech-the-word-that-is-evolves-1077098-1.html (accessed 5 October 2015).

Hong Kong Lawyer (2016), "HKMA Sets up Fintech Office as Regulatory Interest Grows", available at: www.hk-lawyer.org/content/hkma-sets-Fintech-office-regulatory-interest-grows (assessed 10 January 2017).

Institute of Risk Management (IRM) (2002), *A Risk Management Standard*, IRM or Institute of Risk Management, pp. 1-17.

International Standard on Auditing (ISA) (2009), "ISA240: the auditor's responsibilities relating to fraud in an audit of financial statements", available at: www.ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf (accessed 3 December 2016).

Kaiser, T. (2016), "Implications of current changes to OpRisk regulation on banks in Germany", available at: www.iflr.com/Article/3568139/Implications-of-current-changes-to-OpRisk-regulation-on-banks-in-Germany.html (accessed 13 March 2017).

Kellton Tech (2016), "Cyber-attacks: how to protect your financial data", available at: www.kelltontech.com/kellton-tech-blog/cyber-attacks-how-protect-your-financial-data (accessed 21 November 2016).

Kwok, B.K.B. (2005), *Accounting Irregularities in Financial Statements*, Gower Publishing.

Kwok, B.K.B. (2016), *Business Terms and Phrases for Surveyors, Engineers and Facilities Managers in Hong Kong*, Knowledge Conservation, Hong Kong.

Li, M. and Harris, J. (2016), "The Role of Data Science in Fintech", available at: http://blog.thedataincubator.com/2016/08/the-role-of-data-science-in-Fintech/ (accessed 3 December 2016).

McNally, J.S. (2013), "The 2013 COSO framework and SOX compliance", *Strategic Finance*, (June), No. 5.

Manning, W. (2011), "Investigating the clouds", available at: www.fraud-magazine.com/article.aspx?id=4294970016 (accessed 21 November 2016).

Martin, R. (2008), *The Finance Crisis and Rescue: What Went Wrong? Why? What Lessons Can Be Learned?*, University of Toronto Press, Toronto.

Mestchian, P., Makarov, M. and Mirzai, B. (2005), "Operational risk–COSO re-examined", *Journal of Risk Intelligence*, Vol. 6 No. 3, pp. 19-22.

Miller, M.A. (2015), "Faster payments means faster fraud", available at: www.Fintechbusiness.com/blogs/89-faster-payments-means-faster-fraud (accessed 3 December 2016).

Nicoletti, B. (2017), *The Future of FinTech*, Springer International Publishing.

Ng, A. and Ho, F. (2014), "Dynamics of knowledge renewal for professional accountancy under globalization", in Ordóñez de Pablos, P. and Tennyson, R.D. (Eds), *Strategic Approaches for Human Capital Management and Development in a Turbulent Economy*, IGI Global, pp. 264-278.

Ng, A.W. and Mitchell, B. (2009), "Developing knowledge capital in an integrated enterprise risk management system: framework and structured gap analysis for public sector organizations", *International Journal of Learning and Intellectual Capital*, Vol. 6 Nos 1/2, pp. 170-184.

Ng, A.W. and Tang, W. (2016), "Regulatory Risks and Strategic Controls in the Global Financial Centre of China", in Choi, J.J., Powers, M. and Zhang, X.T. (Eds), *International Finance Review – The Political Economy of Chinese Finance*, Emerald Publishing, Vol. 17, pp. 243-270.

Prorokowski, L. and Prorokowski, H. (2014), "Comprehensive risk measure – current challenges", *Journal of Financial Regulation and Compliance*, Vol. 22 No. 3, pp. 271-284.

PwC (2016), "Customers in the spotlight, How Fintech is reshaping banking", available at: www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_11/Accenture-Future-Fintech-Banking.pdf (accessed 21 November 2016).

Rowntree, L. (2016), "How Biometrics in Fintech Can Bring a Different Angle to Using Biometrics in Advertising", available at: www.exchangewire.com/blog/2016/08/18/biometrics-Fintech-can-bring-different-angle-using-biometrics-advertising/ (accessed 3 December 2016).

Taylor Wessing (2016), "Fraud in Fintech: issues, solutions and aspirations", available at: https://united-kingdom.taylorwessing.com/en/insights/corporate-crime-matters/fraud-in-Fintech-issues-solutions-and-aspirations (accessed 21 November 2016).

Treleaven, P. (2015), "Financial regulation of fintech", *The Journal of Financial Perspectives*, Vol. 3 No. 3, pp. 1-14.

Wolters Kluwer Financial Services (2016), "Business Intelligence: a Tech Revaluation for the Evolution in Compliance", available at: www.wolterskluwerfs.com/onesumx/white-paper/business-intelligence.aspx (accessed 21 November 2016).

Zhu, H. and Zhou, Z.Z. (2016), "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China", *Financial Innovation*, Vol. 2 No. 1, p. 29.

Further reading

Eagar, M. (2016), "FinTech + Digital Currency – Convergence or Collision?", *The FinTech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries*, pp. 212-216.

Corresponding author

Artie W. Ng can be contacted at: spartie@speed-polyu.edu.hk