Light at the End of the Shadow: Technology-Driven Banking and Consumer Empowerment

Shadow banking exists to fulfil a market need for both savers and borrowers. In many cases, shadow banking provides banking-type services more efficiently than traditional, regulated banks, but possibly with greater risk. Shadow banking, as defined by UK’s Financial Stability Board, is lending and borrowing by institutions other than the regulated banking system. In most countries, banks are the only authorised depository of savings with last-resort support by the central bank. In return, they are subject to restrictive rules and regulations.

But funds can and do bypass the banks from savers directly to investors. Viewed broadly, shadow banking includes any bank-like activity undertaken but not regulated, including via mobile payment systems, e.g. Vodafone; technology-based bond trading platforms; and investment products sold by Chinese trust institutions. Academic usage is narrower: i.e., forms of credit that closely track what regulated banks do, e.g. direct lending, private equity, investment funds, money and bond markets. However, many bankers regard any encroachment on their business as shadow banking. Shadow banking is a serious business in terms of size, estimated to be 111% of world GDP in 2011, according to the Federal Reserve Bank of San Francisco.

The recent development of internet-based operators entering the banking services industry, such as Alibaba in China, has heightened the possibility not only of higher levels of efficiency and innovation but also of instability. In the case of Alibaba, it entered the banking sphere based on its large-scale B to B and B to C third party payment arrangements. Within ten days in July 2014, Alibaba’s first mutual fund, Yuebao, raised over 500 billion RMB, dwarfing the size of the previous largest mutual fund in China. This emphasises the speed of potential shadow banking growth given current technology. To bring this under control, the Chinese government licenced Alibaba as a banking services provider.

As a general principle, the Asian Shadow Financial Regulatory Committee is of the view that governments should allow the extensive use of technology in banking to promote competition and efficiency, and implement effective monitoring.

For regulators, in the event that specific components of shadow banking are brought within their ambit, they have the responsibility to protect the interests of consumers and other stakeholders.
1. Meaningful disclosure assists consumers and small businesses understand the costs and benefits and risks associated with financial products and services provided by internet banking, so they can make informed judgement about the suitability of any product or service meeting their needs.

2. Competitive market forces are needed to ensure that fees and charges imposed are not excessive, i.e., need to impose best practices on fair and reasonable fees and charges.

3. Pursue broader measures to improve the transparency, integrity, and efficiency of the credit process, especially credit information based on private credit bureaus. To protect the integrity and accuracy of the personal credit information of consumers, regulators should take note of Singapore’s recent Credit Bureau Act aimed at maintaining data confidentiality and security. It proposes to license private credit bureaus to improve the standards for fair credit reporting and provide consumers with free copies of their credit report within a mandated period of a credit application being approved or rejected to bring about greater data purity.

4. Strengthening avenues for consumer redress

There is a need to enhance the regulators’ system of monitoring and better manage risks that could hurt consumers arising from: (i) more complex products/services as a result of continuing pressures on the profitability of financial service providers from internet banking; engaging in bundling of products; and borrowers taking on more debt than they can afford; (ii) the search for higher yields leading consumers to buy new products without properly understanding the risks; and (iii) new delivery channels exposing private information; and possible fraudulent activities.