The Challenges And Disadvantages Of Fintech Revolution

Traditional financial institutions are currently transforming into a new era of innovation, which brings in technology into the new field of financial services (Fintech). Fintech has been growing rapidly since PayPal was first recognized. It brings a bunch of benefits for startups as well as organizations. According to the president of Pintech, A Chinese fintech startup, Zhou Jing, said that the Chinese industry's rise as people are addicted and relying on the mobile phones and applications. In the past, people did not have smartphones and they did not have access to information or services that are readily available if they live far away. Today, without opening a bank branch, we can reach out to customers who live faraway places. People can now provide retail financial products to the majority of the population in China at marginal cost, or close to zero. However, the revolution of financial and banking services industry come along with problems and disadvantages.

First, companies are now facing more dangerous cyber security issues that could affect millions of users. Cyber security is a technique to protect networks, computers, programs, and data from unauthorized access or attacks. Along with all the new technology that has boosted the growth of today's diverse FinTech sector, the number of cyber attacks keep on rising since 2012. According to Equifax, over 143 million accounts were compromised in a massive data breach, in which hackers stole passwords, names, and other important information from account holders back in September of 2017. Although some larger financial institutions have the capabilities to secure their websites, but smaller firms may not because of limited resources. Criminals are now expert at finding weak links in the security chain and once they get in, they can explore other weaknesses to increase their control. In addition, it enables them to have unlimited access and attacks without being detected. Many institutions have numerous security tools that add complexity rather than providing solutions. When these tools do not communicate efficiently, they will not provide the visibility security teams need to establish seamless, holistic protection, which is required to keep up with today’s threats. Distributed denial of service attacks (DDoS) happens when heavy volumes of traffic are gathered at a website to damage normal activity, typically freezing up the site for several hours. Such exploits achieved notoriety in the fall of 2012 when large banks were hit by a cyberterrorist group. According to Verisign’s report, the number of attacks against the financial industry doubled to account for 15% in the fourth quarter of 2014. Other than that, 43% of the bank targets were hit more than six times which stated in Neustar’s report. “Cybersecurity is not very good in China,” statement proposed by Jim Fitzsimmons, a Singapore-based director of the cyber consulting team at Control Risks, who has been helping multinational companies on the Chinese mainland adapt to the regulations. “A lot of information is bought, stolen and traded, so the government wanted to tighten that up.”

To the extent that FinTech activities are innovative and are not covered by existing legislation, legal and regulatory frameworks may need to adapt. . As the growing numbers of FinTech startups, the government has increased the regulations and many of these rules have implications for its technological systems. It means more complex software for monitoring risk and ensuring regulatory compliance. Now, a FinTech business needs to consider at an early stage whether it requires regulatory approval to conduct business. So far, there is no single comprehensive law which regulates the FinTech businesses in China. However, it applies different administrative measures and guidance regarding financial product or services. Other than that, the block chain rule issued by CAC also demonstrated the government's efforts in strengthening the fintech market. According to the Block Chain Rule, all blockchain information service providers must file their business via online management system within 10 days of their provision of service. If the blockchain information service providers fails to file with CAC or submits misleading information when filing, CAC and its local offices may issue a rectification order or, in serious cases, issue a warning and impose a penalty of up to RMB 30,000.

Last but not least, certain FinTech activities could increase third-party reliance within the financial system. For example, cloud computing services could be provided by a limited number of parties, which could have significant implications for a range of cloud-based financial services in the event of operational issues. Disruptions to these types of third-party services, perhaps due to operational difficulties, are more likely to pose systemic risks the more central these third parties are in linking together multiple systemically important institutions or markets. For instance, robo-advice and FinTech lending may rely on a set of third-party data providers that could be highly concentrated. As in the case of retail payments, the third parties may not themselves be traditional financial institutions (e.g. telecommunications).