Digital onboarding in the era of Smart Banking

As part of its efforts to usher in a new era of smart banking, the Hong Kong Monetary Authority (HKMA) has introduced several important measures to encourage the use of financial technology, foster financial inclusion and enhance customer experience in the industry.

In addition, the development of virtual banking in Hong Kong is expected to boost innovation and competition in the retail banking sector. These new players will seek to gain a competitive edge by streamlining the account opening process, providing personalised and round-the-clock financial services and delivering an improved customer experience.

Leveraging their longstanding customer relationships and proven track record of reliability and sustainability, many traditional banks are also developing financial technology and partnering with technology providers to enhance their digital offering. As the industry transitions towards the digitisation of banking services, digital onboarding will soon become the norm.

KPMG highlights six key considerations and practical applications for banks around digital onboarding.

1 Regulatory framework

Regulatory guidelines continue to be refined to support technology and innovation. In the area of anti-money laundering and counter-financing of terrorism (AML/CFT), the revised Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (AMLO Guideline) of October 2018 and the recent HKMA Letter of 1 February 2019[1] provide greater transparency around regulatory expectations with respect to digital onboarding:

- The baseline that customer due diligence (CDD) measures must be conducted before establishing business relationships with customers applies to regular onboarding and digital onboarding.
- Where digital onboarding is applied, a customer is not physically present for identification purposes, and therefore additional measures should apply to mitigate impersonation fraud risk.
- Where technology solutions are adopted, the expectation is that these should be at least as robust as those performed in front of personnel at authorised institutions, and should cover the two key aspects of identity authentication and identity matching.

[1] Hong Kong Monetary Authority, February 1, 2019, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190201e1.pdf

2 Money laundering/terrorist financing risk

With greater transparency of regulatory expectations around digital onboarding, banks should evaluate and understand the associated risks in order to determine the appropriate risk mitigating controls. In line with a risk-based approach to managing money laundering and terrorist financing (ML/TF) risk, banks should consider:

The risk profile of the digital customer

The risk profile of a customer onboarded via digital channels differs from that of a customer on-boarded in a branch due to the risk of impersonation fraud. As fraud cases in Hong Kong appear to be on the rise and account for a good share of predicate crimes of money laundering cases examined,[2] concerns over impersonation fraud in relation to digital channels are well-founded.

When considering appropriate measures to mitigate impersonation fraud risk, banks should:

- Leverage existing mechanisms on fraud prevention (e.g. detection and credit card fraud).
- Use data from multiple sources or incorporate qualitative checks that assess the strength of the information supplied, for example, in addition to information obtained during onboarding.
- Require that additional measures be applied to high-risk customers and customers that are politically exposed persons themselves or are connected to politically exposed persons.

Changes to geographical risk

Digital onboarding inevitably means an expansion of geographical risk as accounts can now be opened from anywhere in the world. Banks could consider augmenting geographical location information obtained in the account opening process with IP address data and GPS location data collected during onboarding, and using this data on the location (city, region, country) in the assessment of geographical risk.

Managing accessibility to products and services

Banks should consider imposing restrictions on the access to products and services via the digitally opened account as an additional level of control. When considering this option, it should be acknowledged that money laundering and terrorist financing do not require sophisticated and complex products. Setting transaction permissions using a tiered approach and applying appropriate thresholds could therefore be useful.

Managing expanded channel risks

A digital platform is in itself a new delivery and distribution channel risk. In addition to impersonation fraud risk, other risks associated with the use of digital channels include cybersecurity and data security (see sections **3** and **4**).

Prompt detection of sanctions and other financial crime risks is critical

With the expansion of geographical risk comes an inherent expansion of customer types. The screening of customers is a risk mitigating measure that needs to be embedded into the digital onboarding journey to identify if a customer is either on a sanctions list, or an individual that has been convicted for – or is suspected to be associated with – money laundering, the financing of terrorism or other financial crime. Digital onboarding of such customers should be terminated upon confirmation that the customer is a sanctioned party and/or is connected to a sanctioned party; whereas mechanisms to ensure thorough review of "suspect" cases prior to proceeding to a next step in the account opening process should also be established. Accordingly, in the assessment of the technology solutions deployed for the purposes of onboarding, the screening mechanisms of customers and their connected parties (including the place in the process, timeliness and ancillary decision making processes) are a vital consideration.

Technology risk: what to consider when technology takes over from human operators

Where technology solutions are used for onboarding, the HKMA Letter of 1 February 2019 sets out the expectations on ensuring the reliability of the documents provided by customers for identification and verification purposes. This includes ascertaining the genuineness of the identity document by using detection of security features of identity documents and procuring to link the customer incontrovertibly to the identity document provided.

Prior to adoption, technology solutions should be tested thoroughly to demonstrate that there is:

- A thorough understanding of the solution's capabilities, including the settings and how these can affect performance;
- An assessment of the risks related to using the solution, including potential system failures and errors in algorithms and logic;
- A backup plan for when the solution does not operate as intended;
- A plan to equip personnel with the right skills and knowledge to support the deployment of the solution;
- Ongoing monitoring and testing of all aspects of the solution to ensure that it is capable to operate as designed; and
- Adequate governance and oversight of the ML/TF risks that may arise as a result of a failure or deficiency of the solution.

Payment channels

Connectivity to digital payment platforms forms part of the services offering, but payment channel risks may sometimes be overlooked in the assessment of ML/TF risk. While digital payment providers are mostly licensed subject to supervision by the HKMA, AML/CFT control requirements are not equivalent to those applicable to banks. Banks facilitating incoming and outgoing funds for and on behalf of their customers should consider the payment channel risks from an overall perspective of the transactional arrangements that take place via the bank account. This includes to what extent the payment channel can be exploited to facilitate the layering of transactions to obscure the source or destination of funds.

2 *'Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report'*, April 2018, https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

3 Data governance

The digitisation of banking products and services means that the quality of data is becoming increasingly critical, not just to mitigate impersonation fraud risk and money laundering risk, but also to obtain better quality insights on customer behaviour.

Many traditional banks face challenges in maintaining the quality of data. The existence of various data sources and inadequate data aggregation, validation and cleansing processes indicates that insights generated from the data have known limitations in terms of being accurate and complete.

This is an area where virtual banks might have an advantage as they start with a clean sheet and are not bound by infrastructure limitations or legacy issues with data quality. The virtual banks will be keen to fill the customer experience gaps left by the traditional banks by leveraging technology solutions to aggregate better data points at a faster speed and with greater accuracy – for example, through the use of machine learning algorithms.

Data acquired via digital onboarding is different to that gathered via in-person onboarding. For example, biometric data and solution-held data with regards to liveness detection are not necessarily obtained during face-to-face onboarding, but are likely to be collected as part of digital onboarding. Banks should therefore enhance their existing data governance frameworks to cater to all the data being collected. Based on this data, analysis can be performed for risk management purposes, for example in the monitoring of suspicious locations, activities, persons and transactions.

A robust data governance programme should include an enterprise-wide data policy at the outset to ensure reasonable, effective and consistent practices across the organisation. A clear and appropriate data governance team should also be in place to facilitate and execute the different workstreams under the programme. Roles and responsibilities must be clearly defined and stakeholders from different lines of business need to be involved in the data governance team. To continuously measure the effectiveness of the data governance programme, corresponding KPIs/KRIs and dashboards should also be agreed for regular review.

In addition to data quality, typical data governance workstreams to support effective risk management for banks would include reference and master data management to ensure that strategically important data is always consistent across analytical and operation systems. They would also include a good metadata management practice to provide a clear data dictionary to both business and technical users. Finally, emphasis must also be placed on modern analytics technology. For example, technology like graph databases will help to determine suspicious activities in AML effectively, despite many levels of separation that commonly exist.

4 Data protection and cybersecurity

As with any other technology, embracing digital onboarding comes with associated cyber risks and privacy issues. These include the circumventing of onboarding controls by cyber criminals, mishandling and risk of leakage of digital profiles by the banks, and cybersecurity risks arising from the integration of existing unsecure infrastructure into digital onboarding solutions.

While the HKMA encourages financial institutions to embrace fintech such as digital onboarding solutions for greater customer convenience, it also expects them to take appropriate action to maintain the cybersecurity of digital onboarding solutions and to protect customer data and privacy. There are a number of steps banks should take as they embrace digital onboarding solutions, including:

- Conducting a thorough evaluation of the security robustness of the onboarding solution.
- Assessing the reliability of the solution developer to support the bank with maintaining security robustness.
- Assessing the IT control environment of the technology service provider if outsourcing is involved.
- Establishing internal checks and balances to ensure onboarding solutions are operated, maintained and monitored appropriately.
- Collaborating with the bank's cybersecurity team to ensure that appropriate actions are taken based on cyber threat intelligence related to the digital onboarding solution.
- Instituting a backup plan in case of a cybersecurity incident.
- Launching a client education programme on the pros and cons of digital onboarding, which should include providing them with alternative onboarding methods.

5 Governance and oversight

Ongoing digitisation in the banking sector requires building and maintaining trust in the entire digital ecosystem. This in turn requires a strong risk culture and leadership at banks to guard against cyber risk and other digital risks. To this end, regulators expect financial institutions to establish proper governance and oversight structures for all technology solutions, including for digital onboarding.

In addition, policies and procedures should be regularly reviewed and amended where necessary, taking into consideration processes and solutions used in digital onboarding. Senior leadership involvement and oversight should ensure that investments are aligned with business objectives, and that digital onboarding solutions are properly integrated into the existing infrastructure to maximise efficiency.

6 Customer experience

The regulatory trends highlighted previously share a common theme of ensuring security while creating a seamless banking experience for customers. Furthermore, with the shift towards open banking, both customers and third party service providers will have more access to and control over their own information than ever before.

How banks, fintech firms and non-banking institutions adapt to this change will become increasingly critical as expectations to enhance data usability and transparency for customers will override the traditional model of retaining as much propriety information as possible in-house.

In addition, 97.5 percent of China's 772 million internet users access services via their mobile devices,[3] with digital no longer a choice, but an expectation for functionality and convenience. Customers are more focused on how digital channels can enrich their banking objectives in an optimal way.

When devising a digital strategy in the era of Open APIs, virtual banks and disruptive technology, banks can choose to Protect, Compete or Innovate (see chart below), depending on which option is most aligned with their objectives to improve digital channel experiences. This should also align with the digital innovation appetite of the business function that manages distribution and customer interaction channels, as well as the strategic vision of the overall organisation.

[3] *'Tomorrow's experience, today'*, KPMG International, June 2018, https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/tomorrows-experience-today-harnessing-a-customer-first-approach.pdf

Your position in adopting digital onboarding

Protect

Develop in-house processes and standards to a level that is compliant with jurisdictional needs (data privacy, API guidelines)

Compete

Invest in strategic enablers both in-house and externally including internal data usage (e.g. unstructured, big data) and external (e.g. mobile app, social media)

Innovate

Build strategic partnerships including with non-FS related parties. Focusing on a model that prioritises customer centricity, data insights and agility while maintaining security and transparency

Key trends observed in other jurisdictions

Business

The Monetary Authority of **Singapore** (MAS) has supported financial institutions' use of technology (**non-face-to-face verification**) to onboard customers, driving better experiences while addressing ML/TF risks.

UK challenger banks use photo ID and smartphone cameras for a '**Liveness Test**'.

Using real-time **biometric traits** for onboarding to combat impersonation risk, a key concern among regulators.

Technology

Korea's leading social media platform launched its own digital bank which enables account opening via the app without visiting a bank, and attracted **820,000+** customers in the first **four days**.

80% of adult **Norwegians** utilise a 'Bank ID' for banking services and account opening. Bank ID is in compliance with EU **Know Your Customer** (KYC) and AML regulation.

Regulations

Mainland China has announced new **AML** and **counter-terrorist financing regulations** for online financial institutions, while setting up control mechanisms for new applications using the **National Identification System** for centralisation.

Australia's open banking regulations require banks to provide phase 1 **API data sharing** by **July 2019**. Preparation of infrastructure and standards being finessed via their new payments platform launched in February 2018 enabling **24/7, real-time payment transactions.**

Sources: Tradelink HK, Finextra 2018, MAS circular AMLD01/2018, Open ID exchange: Digital identity report 2016, RBA NPP 2018, Euromoney Korea's digital banks 2018

Contact us

Paul McSheaffrey
Partner, Head of Banking & Capital Markets, Hong Kong, KPMG China
T: +852 2978 8236
E: paul.mcsheaffrey@kpmg.com

Rani Kamaruddin
Partner, Head of AML & Sanctions, Hong Kong KPMG China
T: +852 2140 2815
E: rani.kamaruddin@kpmg.com

Henry Shek
Partner, Head of IT Advisory Risk Consulting, KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

James O'Callaghan
Partner, Head of Technology Consulting, Hong Kong, KPMG China
T: +852 2143 8866
E: james.ocallaghan@kpmg.com

Tom Jenkins
Partner, Head of Financial Risk Management, KPMG China
T: +852 2143 8570
E: tom.jenkins@kpmg.com

Bhagya Perera
Director, IT Advisory, KPMG China
T: +852 2140 2825
E: bhagya.perera@kpmg.com

Stanley Sum
Director, CIO Advisory, KPMG China
T: +852 2143 8808
E: stanley.sum@kpmg.com

Edwin Hui
Director, Data & Analytics, Management Consulting, KPMG China
T: +852 2847 5009
E: edwin.hui@kpmg.com

Christian Leung
Associate Director, IT Advisory, KPMG China
T: +852 3927 4629
E: christian.leung@kpmg.com

Brian Cheung
Associate Director, IT Advisory, KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

kpmg.com/cn

Publication number: HK-FS19-0001

Publication date: April 2019