The new world in non-face-to-face customer onboarding

The world has changed significantly in the last decade, but customers are largely still onboarded via the old-fashioned physical face-to-face approach and identification verification through sighting of the physical photographic ID by the reporting entity e.g. bank. But is physical face-to-face onboarding that much superior or of lower risk than non-face-to-face onboarding and digital verification? The world is now at an inflexion point where the pros of non-face-to-face onboarding may outweigh the cons – they include health concerns in the era of COVID-19.

In the Financial Action Task Force (FATF) Recommendations 2012 (revised in June 2019 and most recently in October 2020), the FATF still attributes non face-to-face customer onboarding or transactions as typically higher risk. In the interpretive notes to FATF Recommendation 10 on customer due diligence, under the risk category of *Higher Risk, paragraph 15* (*c) Product, service, transaction or delivery channel risk factors,* non-face-to-face relationship is identified as a higher risk factor, together with private banking, anonymous transactions (which may include cash) and payments received from unknown or un-associated third parties. The higher the risk, the greater are the mitigation measures and expenses – which act as barriers to the adoption of non-face-to-face onboarding.

The FATF is changing its message. As recognised in the FATF Guidance on Digital ID issued in February 2020, "*The Guidance clarifies that non-face-to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk*." It is worth mentioning that, as pointed out in the article previously published by the Alliance for Financial Stability with Information Technology (AFS-IT), the FATF policy paper on *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses* in May 2020 highlighted the benefits of Digital KYC during COVID-19.

Nevertheless, for those who know the FATF nomenclature well, FATF interpretive notes are binding on members and associate members (basically all countries in the world except for a few). The two recent FATF policy documents on digital ID and COVID-19 are not binding, but setting standards of best practices.

Thirteen (13) years after the launch of the first smartphone which moved us into the digital world with video calls and high resolution photography, the world is dealing with the fight against COVID-19. The pandemic has had the effect of driving the world, particularly work practices into the digital world. However, this was not the result of the introduction of new technology, but out of the necessity to work remotely – and to sceptical employers and reluctant employees alike – it has worked for many, but definitely not for those whose products and services have very limited capacity to

migrate to the digital world e.g. hospitality, tourism and other services that require face-to-face physical interactions.

Despite the changes wrath 13 years ago as described above, particularly with COVID-19 in 2020, there is still a reluctance to migrate to digital environment, or there are still too many obstacles. A quick tour globally of COVID-19 advisories issued by AML/CFT supervisors highlights this more clearly. There have been more advisories issued by the authorities on increased ML/TF risks because of COVID-19, and less on utilising digital or non-face-to-face onboarding. In some instances where varying degree of flexibility has been permitted, they are mostly temporary and limited to the duration of COVID-19. For example they allowed for greater scope in delayed customer verification.

Digital ID can encompass a spectrum – from biometric to video KYC. To be clear, e-KYC including various forms of biometric ID has been used globally prior to COVID-19, particularly among Fintech disrupters. In the case of verification of identity through video, which allows a video meeting as equivalent to a physical face to face meeting, although with controls such as geo-tagging, is not exactly the same as using a smartphone for biometric verification, a selfie check, or electronic verification of photocopies of documents submitted. That said, some video KYC options have a hybrid approach associated with biometric verification. Video verification in its simplest form is limited globally, but it is growing.

In terms of video KYC, the standing out exception among G7 countries is Germany, and coincidentally the home country of the current FATF President (July 2020-June 2022). Germany's Federal Financial Supervisory Authority (BaFin) in response to the emerging digital landscape permitted, in a 2014 directive, more convenient onboarding for prospective customers of banks and financial services providers. It enabled identification and verification via a live two-way video link with a compliance professional. France and the United Kingdom also allow similar approach in customer on boarding, although with varying accompanying control measures.

Arguably video KYC has its risks (e.g. lower level of assurance) but as part of a spectrum of e-KYC options, it has its usefulness particularly from a financial inclusion perspective. Countries in certain regions including in Asia have adopted a more proactive path in the adoption of e-KYC including video KYC. The following are three examples from Asia leveraging not just e-KYC, but also the business functionalities of the smartphone.

Similar to Germany, the Hong Kong Monetary Authority (HKMA) stood out even before COVID-19. The Anti-Money Laundering and Counter-Terrorist Financing Ordinance

and the Guideline on Anti-Money Laundering and Counter-Financing of Terrorism (For Authorized Institutions), permit on-boarding of customers remotely. The term "remote on-boarding" refers to establishing a business relationship with a customer solely through an electronic channel such as mobile applications or internet. Remote onboarding includes video-conference meetings and even allows financial institutions' customers to send in recorded video, subject to robust risk management measures as required.

The HKMA highlighted again the flexibility available in its *Coronavirus disease (COVID-19) and Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) measures – An Update* on 30 July 2020. The update provided instances of acceptable practices, for example *" ... observed that AIs [*Authorized Institutions*] are increasingly using video conferencing to interact with customers in the course of on-boarding and ongoing customer due diligence reviews.*."

In the Monetary Authority of Singapore's (MAS) Circular No. AMLD/2018 on the use of MyInfo (a service provided by the Singapore Government which enables citizens and residents to manage the use of their personal data for simpler online transactions) as a verified source of identification information, MAS considers MyInfo to be a reliable and independent source for the purposes of verifying the customer's identity. Where MyInfo is used, financial institutions are not required to obtain additional identification documents to verify a customer's identity.

The Circular also highlights the use of non-face-to-face (NFTF) verification measures. Where identity is obtained electronically through other NFTF means, including through transmission of scanned or copy documents, financial institutions should apply additional checks to mitigate the risk of impersonation. The examples include holding real-time video conference that is comparable to face-to-face communication, in addition to providing electronic copies of identification documents.

Bank Negara Malaysia issued a policy document on Electronic Know-Your-Customer (e-KYC) on 30 June 2020. With implementation of e-KYC, a majority of customers will no longer need to visit the physical premises of a financial service provider to open an account. In the new regulation, financial institutions may decide on any combination of methods to conduct identification/verification through e-KYC (e.g. connecting to public or private database, facial recognition, video call), with due regard to the assessment of risk and level of assurance needed for a particular product, provided the requirements in the e-KYC policy document are met.

In summary, some jurisdictions are embracing the digital space more proactively including extending e-KYC to encompass video verification in certain circumstances

because they have assessed that the benefits outweigh the risks, whereas most still tend to maintain the traditional practices while being prudent in accommodating digital driven ones. However, it is believed that a lot more jurisdictions will move towards leveraging not just digital KYC, but also the digital and intelligent functionalities of the smartphones in order to serve the purposes.

AFS-IT

November 2020