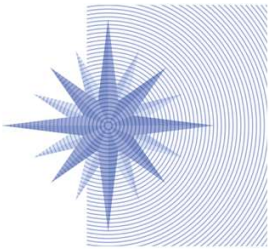

Banco Santander
Bank of America
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JPMorganChase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management

Executive Summary

Customers today expect to engage their financial institution (FI) and manage their finances via their digital device, and prospective customers also increasingly expect to become customers via their digital device. The challenge then to the FI is clear: how to manage the financial crime risks associated with non-face-to-face digital engagement effectively?

Establishing a reasonable and risk-based set of controls is one of the three Wolfsberg Effectiveness Factors, and within that context, the need to prioritise resources and enhance controls.[1] Technology can enable an FI to meet both customer expectations on digital engagement and prioritise resources in an effective, risk-based manner. Digital approaches to customer lifecycle risk management, if defined and calibrated responsibly, provide the FI with an opportunity to build a dynamic understanding of customer risk, refresh relevant customer information on a targeted basis, and pursue new customers – including the financially excluded - without face-to-face interaction while focusing resources to address genuine financial crime threats.

This Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management provides the below considerations for an FI seeking to achieve this ambition:

- Build a more holistic customer profile via a wider concept of identity attributes that complements the elements required under AML/CTF regulation, in line with customer consent and applicable data protection regulation.

[1] https://www.wolfsberg-principles.com/sites/default/files/wb/Wolfsberg%20Group_Demonstrating_%20Effectiveness_JUN21.pdf

- Map the variables behind the holistic customer profile to internal or external data sources capable of alerting the FI to a possible change or deviation from the expected value of any particular data point or attribute.
- Leverage the ability to detect changes and deviations in the customer profile better, so as to evolve from traditional periodic refresh cycles to a more effective trigger-based approach.
- Recognise that reaching the requisite level of robustness on building the underlying customer profile and ensuring adequate assurance levels on underlying systems are both risk-based decisions, where, for example, certain local conditions, including support for financial inclusion initiatives from competent authorities, may warrant distinct approaches to identification, verification, and authentication for certain types of relationships.
- Collaborate with governments on digital initiatives aimed at increasing access to high quality identity data, promoting interoperability, and facilitating access to financial services.

Competent authorities recognise increasingly that with the appropriate controls in place, non-face-to-face customer engagement may be a standard, or even lower-risk engagement channel.[2] The following Guidance describes how digital approaches to building and maintaining a holistic customer risk profile challenge the "added" value of face-to-face engagement for an FI in knowing its customers and assessing the risk they present of facilitating, or engaging in, financial crime.

Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management

1. Introduction

Customers today expect to engage their financial institution (FI) and manage their finances via their digital device, and prospective customers also increasingly expect to become customers via their digital device. These expectations – and the demographics to which they apply – have accelerated and broadened with the coronavirus pandemic, but ultimately, they are founded in the shared recognition, rooted in technology, that when a customer provides due diligence information via secure, digital means to an FI, that customer should be able to access a certain set of financial products. The challenge then to the FI is clear: how to manage the financial crime risks associated with non-face-to-face digital engagement effectively?

The Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management explores how non-face-to-face digital engagement could be considered a standard, or even lower risk channel for an FI by further developing three core AML/CTF controls:

- Expanding concepts of identification and verification, and increasing the emphasis on the importance of authentication;[3]
- Building and maintaining a dynamic, more holistic customer risk profile; and
- Shifting to a targeted, disciplined approach to on-going due diligence by refreshing customer data on a trigger (rather than periodic) basis, dedicating resources effectively to priority risks in real-time.

[2] The principal source here is the Financial Action Task Force (FATF) *Guidance on Digital Identity* (2020).
[3] "Authentication establishes that the claimant who asserts his or her identity is the same person whose identity was obtained, verified, and credentialed during on-boarding". *FATF Guidance on Digital Identity* (2020)

2. Background

The Wolfsberg Group's Statement on Effectiveness[4] identifies, as a principal element of an effective financial crime compliance programme, the need to "establish a reasonable and risk-based set of controls to mitigate the risks of an FI being used to facilitate illicit activity." This Guidance aims to develop this principle further across digital, non-face-to-face management of the customer lifecycle – specifically at onboarding, in assessing customer risk and in refreshing customer data.

As the Financial Action Task Force (FATF) recognised in their *Guidance on Digital Identity*, FIs and government authorities are at an "inflection point" as regards innovation, and with the appropriate controls in place, non-face-to-face customer engagement may be a standard, or even lower-risk engagement channel and can serve as a powerful enabler for financial inclusion.[5] In meeting this challenge, an FI should not see digital customer lifecycle risk management as a competition between physically present and non-physically-present means of customer engagement, but rather as recognition that advances in technology have lessened the traditional importance of a "brick and mortar" office visit for verifying and authenticating the identity and underlying information of a prospective customer. Equally, maintaining an accurate profile of a given customer's risk for facilitating financial crime is less and less reliant on this face-to-face interaction, and increasingly less dependent on customer contact in general.

The guiding principle for an FI in developing a digital customer lifecycle risk management programme is the same as in a traditional programme: building and maintaining, to a reasonable degree, an accurate profile of customer risk. Accuracy here refers to the level of confidence that the information an FI collects is correct and up-to-date – akin to what the FATF refers to as "an appropriate level of trustworthiness,"[6] and that an FI's evaluation of that information allows the FI to predict and respond better to the likelihood of a customer engaging in illicit activity.

Historically, a face-to-face meeting with a customer was an important reference point in the account opening process, a form of human authentication where an FI's employee, with training, would confirm documents as genuine, match a photo of a face on a government ID to the individual present, and implicitly confirm proof of life (now referred to as "liveness detection" with the advent of non-face-to-face channels). Advances in technology have, however, increased the suite of reliable digital reference points now available to an FI to gain this same level of comfort remotely, and at a cost that makes their integration into customer engagement channels feasible across the customer lifecycle. Such technology, when designed and leveraged in a responsible manner, is also often available on an array of smartphone operating systems, opening the door to new, historically underbanked customer segments that purchase their mobile phones second- or even third-hand. These same advances in technology have also increased substantially the level of transparency between an FI and the customer, enhancing an FI's ability to recognise when a customer's risk profile has changed and to update the profile in a timely and effective manner. It is to be noted that, while these advances in technology present an important opportunity for the FI, the following data ethics principles should be considered:

- Design and technical expertise: FIs should understand deeply their underlying technologies and the implications, limitations, and consequences of their use;

[4] See Wolfsberg Statement on Effectiveness
[5] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf
[6] p. 47, *Guidance on Digital Identity* (The FATF, 2020).

- Openness and transparency: FIs need to be open and transparent with customers, regulators, and other stakeholders about how they are using their data; and
- Accountability and oversight: FIs should be accountable to customers, regulators, and other stakeholders for their use of these new "digital reference points" and resulting decisions.

The following sections explore how these new digital reference points map conceptually across three select elements of the customer lifecycle – onboarding, customer risk assessment, and the maintenance and update of customer information during on-going due diligence. The aim is to draw out a series of recommendations for an FI to consider in their application, while recognising that each FI's risk-appetite and resources are distinct. Many of the approaches and technologies described here, which are intended to serve as guiding principles rather than future regulatory expectations, could equally complement face-to-face settings – e.g., analysing the technical device characteristics behind a mobile phone to build a more robust customer profile need not be limited exclusively to digital, non-physically-present onboarding. Even if originally onboarded via traditional methods, building out the customer's digital presence with the FI over the course of the relationship – what the FATF refers to as the customer's "progressive identity" [7] – could aid greatly in the detection of changes to the customer risk profile and subsequent refresh of information. By increasing the application of these digital reference points and understanding the distinct dimensions they represent to the customer profile, an FI can demonstrate how the single reference of the face-to-face engagement no longer provides a material advantage in knowing customers and knowing the risk they present of facilitating, or engaging in, financial crime.

3. Onboarding: more effective identification, verification, and initial authentication, including for financial inclusion

Expanding the scope of identity attributes

Traditional, regulatory-required onboarding information continues to be collected when engaging a prospective customer digitally, often under a series of drop-down questions and answers. But in widening the scope of self-reported data points at the identification stage, the FI is better prepared to leverage more advanced controls across the customer lifecycle. FIs, in this sense, should consider embracing a wider concept of identity that complements often required elements (e.g., date of birth) with expanded attributes or elements (e.g., behavioural biometrics[8] and other identifiers like email address), which will facilitate the FI's ability to build a progressive identity of the customer over time.

Often this expanded information on identity is already collected but not necessarily as part of anti-money laundering and combatting terrorist financing (AML/CTF) regulatory requirements, e.g., an email address or telephone number. Other, more sensitive information linked to the prospective customer's device, such as location data or device identification characteristics, may require consent but does not overburden the onboarding process. Finally, other data points that are neither intrusive nor obvious also enhance the

[7] Progressive identity refers to the customer building a digital presence over time with the FI. As captured by the FATF in their *Guidance on Digital Identity* (2020), "Depending on the jurisdiction's approach to the requirements for proving official identity, digital ID systems can potentially transform the concept of official identity itself, from something that is fixed to something that can strengthen over time—i.e., progressive identity. With progressive identity, as an individual (e.g., the customer) engages in digital financial and other online activities and builds a digital presence, additional identity attributes and authentication factors become available and can strengthen the individual's digital ID, thereby increasing the confidence level in a customer's identity…" (p. 54)

[8] "Behavioural biometric patterns: attributes, based on the new computational social science discipline of social physics, consist of an individual's various patterns of movement and usage in geospatial temporal data streams, and include, e.g., an individual's email or text message patterns, file access log, mobile phone usage, and geolocation patterns". *FATF Guidance on Digital Identity* (2020)

prospective customer's profile and can help prevent fraud, such as how easily the individual navigates the onboarding questionnaire or, for mobile channels, the way in which the individual holds the device in their hand. Given that these elements are often dynamic – they will change or evolve over time as a progressive identity is formed – FIs that aim to leverage these data points will need to structure their systems in a way that both permits and facilitates the regular updating and tracking of the variables behind this holistic customer due diligence (CDD/KYC) profile.

The need for high quality digital identity data

Several private and public sector initiatives (and partnership initiatives) have strengthened the ability to verify key elements of the customer profile substantially by providing direct or indirect access to official government sources on natural persons and legal entities (e.g., date of birth, residency, etc.) as well as the establishment of globally recognised identification information (e.g., the increased adoption of the Legal Entity Identifier or LEI[9]). In this context, the dialogue between the private and public sector on tackling financial crime should include larger strategies on access to high quality identity data, including, but not restricted to, government-supported digital identity and similar accessibility initiatives that promote interoperability among regional, national and local operating systems and facilitate financial inclusion. In some countries, an FI no longer needs to rely exclusively on a government-issued photo identification card handed to a bank teller for inspection but can now leverage an application programming interface[10] (API) to call a government or third-party database (e.g., a corporate registry or voting registry) and verify customer-reported information as correct. Increasingly, similar databases can confirm an individual's professional activity as well.

Services with adequate levels of reliability are now available to confirm the authenticity of a given document, telephone number or email address, or cross-reference the prospective customer's device location against the self-reported address/country of residency. FIs should recognise that reaching the requisite level of trustworthiness on underlying customer data can follow multiple, diverse verification paths, in line with the FI's risk appetite and applicable regulation, as well as local government strategies on financial inclusion.

The initial authentication event

The initial authentication event is a critical element in non-face-to-face digital onboarding, where the prospective customer demonstrates that they are in fact the same person behind the provided customer information, and here too significant enhancements have diminished the traditional importance of physically present onboarding channels.

Real-time video calls or video-selfies, matched with facial recognition, can replace human vision with computer vision and establish a high level of confidence that the individual behind the device during onboarding is in fact the onboarded individual. In real-time the FI is capable of moving through the various prerequisites on identification and verification and straight into authentication: verifying, for example, that the information provided by the prospective customer matches the government-issued photo identification document scanned by the customer's device; validating the authenticity of the document

[9] The LEI is a "20-character, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions." See https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei for more information.

[10] "Application Programming Interface (API): a set of definitions and protocols for building and integrating application software. APIs let digital products or services readily communicate with other products and services". *FATF Guidance on Digital Identity* (2020)

and device via third-party software that meets the FI's assurance standards; and confirming that the photo on the document matches the individual's facial biometric as presented through the device.

However, authentication factors need not be as sophisticated as biometric-based real-time video calls paired with facial recognition. In countries where older generation smartphones (and operating systems) are more prevalent, relying on more advanced inherent authentication factors may be impossible, which should not constitute a barrier to authentication. Other types of inherent factors, along with ownership factors and knowledge factors,[11] when employed together can also provide the necessary level of comfort, recognising that the strength of the initial authentication event does impact confidence in the customer profile, as explored in more depth in the following sections.

4. Dynamic customer risk assessment and the significance of information access

One of the principal opportunities under a digital customer lifecycle risk management programme is the ability to embrace more fully a multi-dimensional, continually updating customer risk profile, drawing for instance on the expanded identification attributes mentioned previously. FIs should leverage this deeper understanding of the customer risk profile, whether the customer is a natural person or legal entity, so as to be more disciplined and targeted in the application of resources to keep information accurate. This would allow for a transition from more traditional periodic refresh cycles to a trigger-based approach (to be addressed in the following section), potentially focusing less on traditional risk factors when, and if, an FI's data indicate that behavioural factors may alert the FI to financial crime risk better.

Traditional customer risk assessment methodologies identify a number of general categories of "risk factors" that inform the overall profile, such as:

- Customer factors (e.g., professional activity, industry sector, legal entity structure);
- Geographical factors (e.g., country of residency/incorporation, area of operations);
- Product, services, and transactional behaviour (e.g., inherent product risk, associated source/destination of funds); and
- Delivery channel (e.g., present or non-present, or via an intermediary).

Under a digital approach, delivery channel is not a "factor among many" to consider, but rather the ordering principle for how an FI manages the customer throughout their relationship with the FI. Here there are two highly relevant variables that increase or decrease substantially the FI's ability to mitigate financial crime risk in a non-face-to-face context: the quality of the initial authentication event at onboarding with the underlying device, and the level of information access to the device afforded to the FI over time.

The authentication event at onboarding, paired with other concepts like binding,[12] establish the initial level of confidence an FI can place on accepting that the observed usage of the device is, in fact, representative of the actual, presumably legitimate behaviour of the customer. When that initial authentication event is not as strong, and thus more susceptible to impersonation/identity fraud – for example authenticating without facial recognition or without a liveness check like a video – that lower

[11] As captured in the FATF's *Guidance on Digital Identity* (2020, p. 22), there are three common approaches to authenticating someone: ownership factors ("something you possess, e.g., cryptographic keys"), knowledge factors ("something you know, e.g., a password"), and inherent factors ("something you are, e.g., biometrics").

[12] Binding: the process of issuing credentials to authenticate that the individual behind the device is in fact the identified/verified individual. *FATF Guidance on Digital Identity* (2020)

level of confidence can extend across the duration of the customer lifecycle unless remedied at a later date. Follow-up authentication events post-onboarding – to be covered in the next section but which can play a very important role in re-affirming confidence in identity – may lose some of their power, as authentication events going forward from onboarding will likely only be as strong as that initial binding. Here an FI should be encouraged to follow its data by mapping identified cases of stolen identity or similar onboarding exploits back to the initial authentication event, where often a clear picture emerges on the underlying level of confidence behind that initial authentication approach.

Particularly critical to the FI's ability to maintain an accurate assessment of customer risk is the level of access granted by the customer to their device data, and the FI's own technical capabilities to leverage that data. For example, a digital delivery channel where the FI has permission to utilise IP address or GPS information behind the customer's device represents a significant level of information access afforded to the FI by the customer that can be used by the FI to inform the customer risk profile better. Alternately, a customer may choose to use a virtual private network (VPN) on a device or block location permission on the FI's app. These are two completely legitimate decisions based on privacy concerns but given the limits these place on the level of information access between FI and customer, the ability of the FI to identify significant deviations in the geographical risk factors mentioned above is diminished. Information access in this regard is not an entry barrier but, given its impact on properly assessing customer risk, it will likely impact the level of necessary customer engagement.

5. On-going due diligence: trigger-based refresh

In order to build an appropriate trigger-based approach for maintaining accurate customer data, the FI should consider de-constructing each broad risk factor, e.g., geography, or transactional behaviour, into a series of variables, or data elements, and map those elements to the internal or external data sources capable of indicating where there may be a deviation from what is otherwise expected from any particular data point (e.g., as collected at onboarding). For example, the traditional country of residence risk factor could map to IP address, which would trigger an alert when the customer spends a significant amount of time outside of their previously reported country of residence. Established thresholds against the variable's behaviour would determine whether or not a deviation reflects a possible change in the overall risk factor and if a specific action is necessary to gain further confidence that the risk profile has actually changed (i.e., the trigger). Initially these thresholds may be theoretical (or vendor-driven based on their experience in applying their tools in working with other FIs), but over time insights drawn from the digital customer lifecycle risk management programme would facilitate the FI's ability to "follow their data" and decrease or increase the need to trigger a specific action.

FIs should further consider that the specific action in responding to the anomaly be anchored in their degree of confidence that the underlying risk factor may have actually changed. For example, if behavioural monitoring indicates that the user of the device has changed hands and now holds the device at a distinct tilt, or has started copying and pasting passwords or basic data into required forms on a webpage (often referred to collectively as "behavioural biometrics"), suggesting perhaps that the individual behind the device is no longer the originally identified and verified individual, this may warrant a low-level authentication event, such as answering a personal question, or re-entering a pin. Where this is completed successfully, it re-affirms confidence that the individual remains the originally identified and verified individual, allowing the FI to understand the appropriate thresholds on behavioural monitoring better. Alternately, if a device's location data indicate that the customer has been in a country outside of

their stated country of residence for a significant period of time, as in the example above, and an API call to a government database confirms that the customer is no longer resident, the customer's risk profile can be updated automatically and the FI can confirm that the trigger threshold was properly set.

This chain of events and feedback – a risk factor deconstructed into observable activities, thresholds on observable activities that indicate possible changes in the risk factor, and targeted action that confirms a suspected change in the risk factor as an actual change – should be explicit, regularly subject to calibration, and assessed for their trustworthiness according to similar criteria applied at onboarding and in assessing initial customer risk. The significant execution risk that such a process generates must be recognised by the FI and mitigated appropriately, and always with a clear understanding of the assumptions that the FI makes in each decision it undertakes, recalling, for example, that:

- Confidence in the decision to modify a risk factor based on an API call to a third-party database is directly related to the FI's confidence in that process and the quality of information within;
- An authentication event to reconfirm the individual is the same as at onboarding is only as believable as the initial authentication strength at onboarding; and
- Monitoring the location of a device to understand if the country of residence of a customer has changed, as an example, is highly dependent on the level of access granted by the customer to underlying device information.

When the decision logic behind a given event chain maintains a high degree of confidence, "trigger refresh" could be largely invisible to the customer; but as confidence decreases, additional measures, including customer contact, may be necessary.

6. Conclusions

The inflection point is clear: non-traditional, often new data points and innovative controls now enable an FI to define various, alternative customer engagement paths beyond the traditional "brick and mortar" office visit. These alternate, non-face-to-face digital paths can ultimately lead to a commensurate level of confidence in the identified and verified customer at onboarding and over the course of their relationship with the FI, provide a deeper, dynamic understanding of the customer risk profile, and permit the FI to be more disciplined and targeted in the application of resources to keep information accurate – moving away from traditional periodic refresh cycles to a trigger-based approach.

In seeking to transition from traditional to more innovative mechanisms in the customer lifecycle, FIs should consider the following:

- Build a more holistic customer profile via a wider concept of identity that complements elements required under AML/CTF regulation with additional identity attributes (often used to prevent fraud or cybercrime), always in line with customer consent and applicable data protection regulation.
- Map the variables behind the holistic customer profile to internal or external data sources capable of alerting the FI to a possible change or deviation from the expected value of any particular data point or attribute, and structure data and the FI's systems architecture in a way that facilitates the regular updating and tracking of these variables under a risk-based approach.
- Recognise that reaching the requisite level of trustworthiness on building the underlying customer profile is a risk-based decision, where, for example, certain local conditions, including support for

initiatives from competent authorities on financial inclusion, may warrant distinct approaches to identification, verification, and authentication.

- Develop a robust assurance strategy focused on the key dependencies upon which the FI's digital customer lifecycle risk management approach is based, assessing their reliability in line with existing frameworks and standards.
- Collaborate with competent authorities on digital initiatives aimed at increasing access to high quality identity data, including, but not restricted to, government-supported digital ID and similar accessibility initiatives that promote interoperability and facilitate access to financial services.
- Embrace as a design principle the recognition that using innovative technology for customer lifecycle risk management should be responsible — i.e., that the design and use of the technology is fit for purpose, secure, reliable, privacy preserving, consent based and accessible to consumers, and complies with relevant regulatory and policy requirements.

Establishing a reasonable and risk-based set of controls is one of the three Wolfsberg Factors from the Group's Statement on Effectiveness, and within that context, the need to prioritise resources and enhance controls. Technology can enable an FI to both meet customer expectations on digital engagement and prioritise resources in an effective, risk-based manner. Digital approaches to customer lifecycle risk management, if defined and calibrated responsibly, provide the FI with an opportunity to build a dynamic understanding of customer risk, refresh relevant customer information on a targeted basis, and pursue new customers without face-to-face interaction – including the underbanked – while focusing resources to address priority financial crime threats.