BERMUDA MONETARY AUTHORITY

Customer Due Diligence/ Ongoing Monitoring FAQs

1. **Does the Bermuda Monetary Authority (Authority or BMA) recognise varying levels of Politically Exposed Persons (PEPs)?**

The Authority's AML/ATF framework supports a risk-based approach which recognises the level of exposure and risk that differs among PEPs in or from Bermuda (domestic), foreign PEPs, and PEPs of international organisations.

Regulated Financial Institutions (RFIs) must treat all foreign PEPs as high-risk and apply Enhanced Due Diligence (EDD). PEPs in or from Bermuda must first be risk assessed by the RFI. Where assessed as higher risk, RFIs must apply full EDD measures, as with foreign PEPs. For foreign PEPs, even after leaving office, a risk assessment should be conducted to determine their level of influence.

2. **Can an entity be considered a PEP?**

As outlined in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, only natural persons can be considered PEPs. However, an entity owned or controlled by a PEP or a close associate may present a similar risk. Therefore, the RFI should apply a risk-based approach to assess the relationship between the entity and a PEP and implement EDD measures where appropriate.

3. **Can a spouse or close associate of a PEP be assigned a different risk rating than the PEP themselves?**

An RFI should consider, on a risk-based approach, whether a spouse or a close associate of a domestic PEP should be assigned a different risk rating than the PEP themselves and ensure the rationale is documented.

4. **Can Simplified Due Diligence (SDD) be applied where the entity is a subsidiary of an RFI or if the entity is a subsidiary of a listed entity on an appointed stock exchange?**

An RFI may apply SDD only where the business relationship or transaction presents a lower risk of money laundering or terrorist financing. Regulation 10 specifies categories of customers for which SDD may be appropriate, including companies listed on an appointed stock exchange and, in certain cases, subsidiaries of such companies or of RFIs.

However, the Regulation also requires that RFIs first assess the risk of the relationship. This means a subsidiary must undergo a full risk assessment and satisfy standard Customer Due Diligence (CDD) requirements before SDD can be applied. Importantly, SDD is not automatic; it may only be adopted where the RFI can demonstrate, on a risk-sensitive basis, that the relationship meets the low-risk threshold outlined in Regulation 10.

5. **Are all CDD documents required to be certified?**

Certification is generally necessary only for key identification documents (such as passports/driver's licences), where additional proof of authenticity is required. This is particularly important in cases:

- Where the RFI cannot examine the document in person (e.g., non-face-to-face onboarding
- Where higher assurance of document integrity is necessary (e.g., high-risk customers, remote onboarding); or
- When dealing with PEPs or when the RFI presents other high-risk factors

6. Is electronic verification permitted for CDD documents, such as a passport and proof of address?

Electronic verification is permitted for CDD documents, including passports and proof of address. However, there are a few conditions, including:

- Institutions must ensure the electronic checks are reliable and independent through risk assessment and testing
- Monitoring the third-party tool to ensure its suitability
- There must be adequate safeguards to mitigate impersonation risks
- The provider used for electronic verification must meet data protection and cybersecurity standards
- Records of the verification process must be retained and auditable

7. Has the BMA provided written guidance on approved third-party digital verification providers (for identification and proof of address)?

The BMA does not maintain a list of approved third-party digital verification providers, as the Authority does not prescribe which service providers an RFI must use to fulfil its regulatory obligations.

Instead, the Authority's guidance specifies that RFIs must utilise a reliable, independent digital identification verification application or tool that is sufficiently safeguarded against both internal and external manipulation or falsification to mitigate the risk of creating false identities. As noted in Question 6, RFIs must also ensure that any digital verification tools employed are subject to appropriate risk assessment, testing, and ongoing monitoring.

8. What procedures and controls are required for verifying customer identity in non-face-to-face onboarding?

As outlined in the Proceeds of Crime (Anti-Money Laundering and Anti- Terrorist Financing) Regulations 2008, EDD is required for clients who are not physically present at onboarding. RFIs must conduct a risk assessment that considers the increased potential for anonymity and impersonation and implement appropriate measures to mitigate these risks.

For non-face-to-face business that is not considered high risk, verification procedures may include passport verification software, digital virtual meetings, and reliable, independent, digital identification systems. For general guidance on non-face-to-face identification and verification, see paragraphs 5.25 through 5.29 of the General Guidance Notes for AML/ATF Regulated Financial Institutions.

Non-face-to-face onboarding is permitted; however, it requires enhanced procedures and controls to mitigate the higher risk of impersonation and fraud. RFIs should adopt one or more of the following:

- Ensure that additional data, information or documents establish the customer's identity
- Take supplementary measures to verify or certify the documents supplied; or
- Require confirmatory certification by an AML/ATF RFI (or equivalent institution) that is subject to equivalent regulations; or
- Ensure that the first payment is carried out through an account opened in the customer's name with a reputable banking institution

9. What constitutes sufficient evidence of ongoing monitoring (i.e., proof of initial screening, ongoing screening)?

As outlined in the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, sufficient evidence of ongoing monitoring includes reviewing business relationships at a predetermined frequency based on a specific review schedule with corresponding risk ratings (e.g., high, medium and low). Ongoing monitoring may also be triggered by an event outside of the frequency review schedule.

An RFI must document the evidence of ongoing monitoring within the customer risk rating form and include a reassessment of the business's relationship risk rating. The assessment typically includes the following:

- Review transactions to ensure they align with the customer's known profile, including source of funds or digital assets, if necessary
- Investigate and document the background and purpose of complex, unusually large, or suspicious transactions
- Keep CDD records and findings up to date, as far as practicable

10. Are RFIs required to maintain systems that automatically monitor and update expired CDD documentation, or may updates be conducted according to the institution's scheduled review cycle?

RFIs are not explicitly required to maintain systems that automatically monitor and update expired CDD documentation. However, RFIs must ensure that:

- CDD information is kept up to date and relevant
- Reviews are conducted periodically and/or based on a trigger by specific events, such as changes in ownership, control, or risk profile; and
- The institution can demonstrate that its review cycle is appropriate to the risk level of the customer

11. Are RFIs required to collect data on the gender of their customers?

RFIs are not explicitly required to collect data on the gender of their customers as part of standard CDD procedures. The Authority mandates that RFIs collect and verify identification information such as:

- Full legal name
- Date of birth
- Principal residential address
- Nationality
- Official identification number (e.g., passport or national ID)