**COURSEWORK 2**

**KEY REQUIREMENTS IN 4AMD RELATING TO THE ON-BOARDING PROCESS**

In finance, client on-boarding is an entire process which users undergo when establishing a business relationship with an obliged entity or relevant person. Obliged entities or relevant persons are not just financial institutions banks etc. They are as provided in the first paragraph of Article 2 of Directive (EU) 2015/849 of the European Parliament and of the Council or in Part 2, Section 8, paragraph 1(2) of the Money Laundering, Terrorist Financing and Transfer of Funds (information of the Payer) UK Regulation 2017 include: ‘

1. Credit institution;
2. Financial institution;
3. The following natural or legal persons acting in the exercise of their professional activities:
   1. Auditors, External Accountants, Tax Advisors;
   2. Notaries and Other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
4. Buying and selling of real property or business entities;
5. Managing of client money, securities or other assets;
6. Opening or management of bank, savings or securities accounts;
7. Organisation of contributions necessary for the creation, operation or management of companies;
8. Creation, operation or management of trusts, companies, foundations or similar structures;
   1. Trust or company provider not already covered under point (a) and (b);
   2. Estate agents;
   3. Other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR10,000 or more whether the transaction is carried out in a single operation or in several operation which appear to be linked;
   4. providers of gambling services.’[[1]](#footnote-0)

In on-boarding a client, there are some key requirements in the process that any obliged entity or relevant person must consider.

First, it must not allow the client keep anonymous account or anonymous passbook[[2]](#footnote-1). this presupposes that when a customer comes into a bank for instance with the request to establish a business relation with it such as opening of a bank account, it must ensure that such a customer gives a name as specified in his identity card. It also means that such name should be a name that can be traced to a particular document or to a person. This is for the purpose of ensuring that the identity of the client or customer is known, be verified and can be referred to in times of risk assessment, monitoring or detection of any money laundering and terrorist act. Anonymous account poses a hindrance to the application of the rules of identification and verification and it will render a relevant person unable to effectively comply with their due diligence obligations and distort their internal control measures.

It has been identified by United Nations Office on Drugs and Crime (UNODC) that one of the stages of money laundering involves using anonymous shell account ( an account that conducts no real business).[[3]](#footnote-2) To prevent money laundering and terrorist financing, the existence of anonymous account must not be allowed.

Second, it must apply customer due diligence (CDD) by ‘identifying the customer; verifying the customer’s identity based on the documents supplied, data or information obtained from a reliable and independent sources which is independent of the customer or client.’ Also, ‘information about the purpose and the intended nature of the relationship should be obtained and assessed.[[4]](#footnote-3) In the process of applying due diligence, the customer’s information must be checked against the documents provided by him or against the information got from a third party. It also means that CDD must “take place before the establishment of business relationship with any client or before the carrying out of transaction.”[[5]](#footnote-4) ‘This may not apply to notaries, other legal professionals, auditors, external accountant, and tax advisors provided they can defend the client.’[[6]](#footnote-5) In some cases, ‘the client may be allowed to open an account but cannot carryout transaction until CDD requirements are complied with.’[[7]](#footnote-6)

In the case of a company, ‘the identity, name, the registration number or other registration number, the address of its registered office and if different, its principal place of business, the law governing the company, its memorandum of association or other governing documents, the names of the board of directors or members of its management body and its senior management[[8]](#footnote-7) must be obtained and verified.’[[9]](#footnote-8)

This means that when carrying out CDD for a company, the company’s name and the number with which it is registered must be checked against the document it provided or from the information supplied by the third party whose information are reliable.

‘When the client or customer is beneficially owned by another person, the relevant person must identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner so that the relevant person is satisfied that it knows who the beneficial owner is.’[[10]](#footnote-9)

‘If the beneficial owner[[11]](#footnote-10) is a legal person, trust, company, foundation or similar legal arrangement, the relevant person must take reasonable measures to understand the ownership and control structure of the legal persons, trust, company, foundation or legal arrangement.’[[12]](#footnote-11)

If the customer is a body corporate and the relevant person has not succeeded in identifying the beneficial owner of the company or has doubt whether the individual identified is in fact the beneficial owner, the relevant person may treat the senior person responsible for managing the customer as its beneficial owner but ensure to keep records of all actions it has taken to identify the beneficial owner of the body corporate.[[13]](#footnote-12)

When another person purports to act on behalf of the customer, the person’s identity must be verified and he has to prove that he is authorised to act on behalf of the customer, as well as be identified on the basis of documents or information obtained from a reliable source which is independent of the person and the customer.[[14]](#footnote-13)

This is for the purpose of risk assessment and mitigation of risk arising from money laundering or terrorist financing as well as ensuring the integrity of the financial system.

Third, if the customer is suspected to commit an offence under section 21D of the Terrorism Act 2000 or section 333A of the Proceeds of Crime Act 2002, the relevant person is expected to make such disclosure as contained Part 3 of the Terrorism Act 2000(d) or Part 7 of the Proceeds of Crime Act 2002(e).[[15]](#footnote-14)

This is to ensure the proper tracking of the activities of money laundering and terrorist financing and to absolve the relevant person of complicit.

Fourth, the obliged entity must continue to conduct ongoing monitoring of the business relationship including the scrutiny of transaction undertaken throughout the course of that relationship to ensure that the transaction being conducted are consistent with the obliged entity’s knowledge of the customer, the business and the risk profile for ML/TF purposes.[[16]](#footnote-15)

For instance, for a financial institution, if the customer still has an account with it, the financial institution must continue to cross-check every transaction, update the information of the customer and ensure that what it knows about the customer still align with the information provided by or obtained about the customer.

Fifth, ‘in respect of a “politically exposed person (PEP) or family members or known close associates of PEPs”[[17]](#footnote-16), an obliged entity shall obtain “senior management” approval for establishing business relationship with such person and take adequate measure to establish the source of wealth and source of fund that are involved in the business relationship or transaction and conduct enhanced CDD[[18]](#footnote-17) and ongoing monitoring of those business relationships.’[[19]](#footnote-18)

The Treasury Department of the United State of America said on Friday June 12, 2015 in its National Money Laundering Risk Assessment that “approximately $300 billion is laundered annually”. With the help of these requirements, it is believed that the activities of money laundering and terrorist financing will be reduced.

Also, “beneficial ownership rules are actually good for business because they would lead to reduced corruption and increased competitiveness. It allows banks and other companies to know who they are doing business with and minimise their financial exposure to others’ misdeed” - Mary Beth Goodman, a former member of the National Security and International Policy Team at the Centre for American Progress wrote in American Banker.[[20]](#footnote-19)

**Bibliography**

* Brooke Satti Charles, It All Comes Out In The Wash: The Most Popular Money Laundering Methods in Cybercrime (May 11, 2016) <https://www.securityintelligence.com/it-all-comes-out-in-the-wash:the-most-popular-money-laundering-methods-in-cybercrime>.
* Directive (Eu) 2015/849 Of The European Parliament And Of The Council of 20 May 2015.
* The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

1. Directive (EU) 2015/849 of the European Parliament and of the Council Article 2(1); Money Laundering, Terrorist Financing and Transfer of Funds (information of the Payer) UK Regulation 2017, 8(2). [↑](#footnote-ref-0)
2. Directive (EU) 2015/849 of the European Parliament and of the Council Article 10(1) [↑](#footnote-ref-1)
3. Brooke Satti Charles, It All Comes Out In The Wash: The Most Popular Money Laundering Methods in Cybercrime (May 11, 2016) <https://www.securityintelligence.com/it-all-comes-out-in-the-wash:the-most-popular-money-laundering-methods-in-cybercrime>. [↑](#footnote-ref-2)
4. Directive (EU) 2015/849 of the European Parliament and of the Council, art 13(1); Money Laundering, Terrorist Financing and Transfer of Funds (information of the Payer) UK Regulation 2017, 28(2) [↑](#footnote-ref-3)
5. Directive (EU) 2015/849, art 14(1) [↑](#footnote-ref-4)
6. Directive (EU) 2015/849, art 14(4) [↑](#footnote-ref-5)
7. Directive (EU) 2015/849, art 14(3) [↑](#footnote-ref-6)
8. “senior management” means an officer or employee of the relevant person with sufficient

   knowledge of the relevant person’s money laundering and terrorist financing risk exposure,

   and of sufficient authority, to take decisions affecting its risk exposure. Regulation 19(7). [↑](#footnote-ref-7)
9. Money Laundering, Terrorist Financing and Transfer of Funds (information of the Payer) UK Regulation 2017, Regulation 28(3) (a)-(e) [↑](#footnote-ref-8)
10. Regulation 28(4) (a)-(b) [↑](#footnote-ref-9)
11. “beneficial owner” means the individual who ultimately owns or controls the entity or on whose behalf a transaction is being conducted. Regulation 2017 6(9). [↑](#footnote-ref-10)
12. Regulation 28(4) (c) [↑](#footnote-ref-11)
13. Regulation 28(6)-(8) [↑](#footnote-ref-12)
14. Regulation 28(10) [↑](#footnote-ref-13)
15. Regulation 28(15) (b)-(c) [↑](#footnote-ref-14)
16. Directive (EU) 2015/849, art 13(1) point d [↑](#footnote-ref-15)
17. “politically exposed person” or “PEP” means an individual who is entrusted with

    prominent public functions, other than as a middle-ranking or more junior official;

    “family member” of a politically exposed person includes—

    (i) a spouse or partner of that person;

    (ii) children of that person and their spouses or partners;

    (iii) parents of that person;

    “known close associate” of a politically exposed person means—

    (i) an individual known to have joint beneficial ownership of a legal entity or a legal

    arrangement or any other close business relations with a politically exposed person;

    (ii) an individual who has sole beneficial ownership of a legal entity or a legal

    arrangement which is known to have been set up for the benefit of a politically

    exposed person. Regulation 35(12) (b)-(d). [↑](#footnote-ref-16)
18. In any case identified as one where there is a high risk of money laundering or terrorist

    financing by the relevant person when taking appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject or in information available to the relevant person as provided by its supervisory authority.

    In any transaction or business relationship with a person established in a high-risk third country.

    In relation to correspondent relationships (providing banking or credit services to someone in a third country).

    If a relevant person has determined that a customer or potential customer is a PEP, or a

    family member or known close associate of a PEP.

    In any case where a customer has provided false or stolen identification documentation or

    information on establishing a relationship.

    In any case where a transaction is complex and unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose, or in any other case which by its nature can present a higher risk of money laundering and terrorist financing. Regulation 33(1) (a)-(g). [↑](#footnote-ref-17)
19. Directive (EU) 2015/849, art 20 point b, i-iii [↑](#footnote-ref-18)
20. Brooke Satti Charles, It All Comes Out In The Wash: The Most Popular Money Laundering Methods in Cybercrime (May 11, 2016) <https://www.securityintelligence.com/it-all-comes-out-in-the-wash:the-most-popular-money-laundering-methods-in-cybercrime> [↑](#footnote-ref-19)