Regulation No. 4

On Due Diligence of the Customers of the Entities Carrying Out Financial Activities on a Professional Basis

THE FINANCIAL INFORMATION AUTHORITY

having regard to the Law No. XVIII on "*Transparency, Supervision and Financial Intelligence*", of 8 October 2013, and in particular Articles 9 (2) (b) (v) (viii), 13, 22 (3), 24 (2) and 25 (2) (3) on due diligence;

whereas:

the Financial Information Authority, on the basis of the general risks assessment, is entrusted with identifying, by regulation, the sectors and typologies of relationship, product, service, operation, transaction and channels of distribution of low risk, pursuant to the Article 13 (1) of the Law No. XVIII of 8 October 2013;

the Financial Information Authority is entrusted with identifying cases of applicationof simplified and enhanced customer due diligence, and with indicating the procedures and measures to be adopted, including the requirements to be fulfilled, pursuanto to the Articles 9 (2) (b) (v) (viii), 13 (2), 22 (3), 24 (2) e 25 (2) (3) of the Law No. XVIII of 8 October 2013;

the Financial Information Authority is entrusted with supervising and verifying the fulfilment, by the supervised entities, of the obligations established in the Title II of the Law No. XVIII of 8 October 2013, including Chapter III on customer due diligence, the related obligations established by the regulations, and the guidelines, adopted by the Financial Information Authority itself, pursuant to the Article 46 (a) of the same Law No. XVIII;

the Financial Information Authority is entrusted with sanctioning the violations or systemic non-fulfilment of the obligations established in Title II of Law No. XVIII of 8 October 2013, including Articles from 15 to 30, and related obligations adopted by the Financial Information Authority itself, pursuanto to the Article 47 (c) of the same Law No. XVIII.

Giving execution to the decision of the Board of Directors of 19 September 2018

PROMULGATES THE FOLLOWING REGULATION

Title I

Scope of application, criteria of application and definitions

Article 1. *Scope of application.*

This Regulation applies to entities carrying put financial activities on a professional basis.

Article 2. *Criteria of application.*

The provisions of this Regulation shall be applied consistently:

a) with the institutional, legal, economic, commercial and professional framework of the State;

b) with the principle of proportionality, by taking into account operational size and complexity, the nature of the financial activity carried out, the type of services provided, as well as the economic and financial setting and macroeconomic conditions under which supervised entities carry out their activities.

Article 3. *Definitions.*

For the purpose of this Regulation, the following definitions shall apply:

1. « *Suspicious activity* »:

a) an activity that leads to have the suspect or reasonable grounds to suspect, that funds or other assets are the proceeds of criminal activities, or are linked or related to the financing of terrorism or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism;

b) activities, including professional and economic activities, operations or transactions which supervised entities consider particularly likely, by their own nature, to have a link with money-laundering or the financing of terrorism or with terrorist organizations or those who finance terrorism.

2. « *Public authority* »: organ or body of the Holy See or the State.

3. « *Shell bank* »: a financial or credit institution that has no physical presence in the State in which it is incorporated and authorized to carry out its activity and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision.

4. « *Category and status of the customer* »: classification of customers taking into account the category to which they belong (natural persons or legal entities;) and status (for example, ecclesiastic or lay people; dignitaries of the Catholic Church; Politically Exposed Persons; etc.); categories may be divided in one or more sub-categories (for example, natural persons: employees of the Holy See or the State; legal entities: governmental bodies of the Holy See or the State; non-governmental bodies of the Holy See or the State; Institutes of Consecrated Life and Societies of Apostolic Life; Dioceses and Parishes of the Catholic Church; non-profit entities; etc.).

5. « *Correspondent accounts* »: the accounts held by financial institutions, normally on a bilateral basis, for the provision of inter-bank services, like the remittance of drafts, cheques, money orders, transfer of funds, remittance of documents and other transactions.

6. « *Payable-through accounts* »: correspondent accounts that are used directly by third parties on their own behalf.

7. « *Dormant account* »: an account on which no operations or transactions are registered for a period of 10 years.

8. « *Counterparts* »: financial institutions with whom the supervised entities have relationships for carrying out authorized financial activities.

9. « *Identification data* »:

a) natural persons:

i) name and surname;

ii) place and date of birth;

iii) nationality;

iv) State and place of residence or domicile (if different from residence);

b) legal entities:

i) name;

ii) date of incorpopration and registration;

iii) State of incorporation and registration;

iv) legal office or main operational office (if different from the former).

10. « *Personal data* »: any information relating to an identified or identifiable natural person.

11. « *Currency* »:

a) currency, including banknotes and coins that are in circulation as a means of exchange.

b) bearer negotiable instruments, including monetary instruments in bearer form such as traveller's cheques; negotiable instruments, including cheques, promissory notes and money orders, that are either in bearer form, endorsed without restrictions, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments, including cheques, promissory notes and money orders, signed, but with payee's name omitted.

12. « *Identity document* »: an authentic and valid identity document, and in particular:

a) identity card;

b) passport (ordinary, service, or diplomatic); or

c) the following equivalent documents:

i) driving license;

ii) identification cards;

provided they are intacts, legibles, and with a photograph of the holder.

A document is « *authentic* » if issued by the competent Authority of the Holy See or the State, or of the issuing foreign State.

A document is « *valid* » if the expiry date is later than that in which it is presented to the ends of the due diligence.

13. « *Non-profit entities* »: associations or foundations that primarily engage in raising and/or distributing funds for charitable, religious, cultural, educational, social or humanitarian purposes, as defined in Article 1 (3) of the Law "*On registration and supervision of non-profit entities*", No. CCXI of 22 November 2017.

14. « *Supervised entities* »: entities carrying out financial activities on a professional basis.

15. « *Family members* »:

a) the spouse of a politically exposed person;

b) the children of a politically exposed person and their spouses;

c) the parents of a politically exposed person.

16. « *Risk factors* »: variables that, either on their own or in combination, may increase or decrease the money laundering or terrorism financing risk posed by an individual relationship or occasional transaction.

17. « *Financing of terrorism* »:

a) the acts set forth in article 23 of "*Law on supplementary norms on criminal law matters*", No. VIII of 11 July 2013;

b) participation in acts established by article 23 of "*Law on supplementary norms on criminal law matters*", No. VIII, of 11 July 2013, association to commit such acts, the attempt to perpetrate them, the fact of assisting, instigating or advising someone to commit them or the fact of facilitating their execution.

18. « *Funds* »: assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and any legal documents or instruments, including electronic or digital, evidencing title to, or interest in, such assets.

19. « *Funds or other assets* »: any assets, including financial, economic and any other assets, whether tangible or intangible, movable or immovable, however acquired, and any legal documents or instruments, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including bank credits, traveller's cheques, cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

20. « *Operational functions* »: functions directly involved in carrying out of the main activities of the supervised entity, including services and relations with customers, which are entitled to "line controls", or "first level controls", in order to ensure compliance with the regulatory framework in force in carrying out operations. This also through units dedicated exclusively to control tasks with direct reporting to heads of the operating structures, or through controls carried out within the "back office".

21. « *Nature and purpose of the relationship* »: classification of the ongoing relationships based on their nature (for example, personal account of a natural person; or institutional account of a legal entity) and main purpose declared by the customer (for example, crediting of salary; etc.); the categories elated to the nature of the ongoing relationships may be composed of one or more sub-categories (for example, governmental institutional account; or non-governmental institutional account, etc.).

22. « *Person who is entrusted with prominent public functions* »:

a) heads of State or of Government, Ministers and their deputies, Secretaries-General and persons with analogous functions;
b) members of Parliaments;

c) members of Supreme Courts, of Constitutional Courts and of other high-level judicial organs whose decisions are not normally subject to appeal, except in extraordinary circumstances;

d) members of Courts of account and the Boards of Central Banks;

e) ambassadors and *chargés d'affaires*;

f) Senior Officers of the Armed Forces;

g) members of management, administration or boards of State-owned corporations;

h) analogous functions within the Holy See and the State.

i) members of the governing bodies of political parties;

j) general secretaries, directors, deputy directors and members of the governance bodies of an international organization.

23. « *Legal entity* »: any legal entity, whatever the nature and activity, including companies, foundations, non-profit entities and trusts.

24. « *Politically exposed person, PEP* »: a person who is or has been entrusted with a prominent public function in the Holy See, in the State or in any other State or in an international organization. The definition of politically exposed person does not cover middle ranking or more junior officers.

The Finanacial Information Authority publishes and regularly updates list of the functions that within the Holy See and the Vatican City State are qualified as politically exposed persons.

25. « *Payment services provider* »: natural persons or legal entities whose activity includes the provision of payment services or transfer of funds.

26. « *Economic profile* »: profile attributed to the customer on the basis, inter alia, of the nature and purpose of the relationship, the typology of requested products or services, expected operations, customer's economic and financial situation, taking into account the category and status of the customer.

27. « *Risk profile or customer's effective risk (CER) profile* »: the effective risk the customer is posing to the supervised entity, defined on the basis of the different risk factors and parameters.

28. « *Relationship* »: ongoing relationship of an economic, commercial or professional nature, which may be connected to the activity carried out professionally by a supervised entity and which from the moment of its establishment is presumed to have some duration.

29. « *Correspondent relationship* »:

a) the provision of financial services by one financial institution (correspondent) to another financial institution (respondent), including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;

b) the relationships between and among financial institutions and credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

30. « *Contact details* »:

a) natural persons:

i) address of residence and domicile (if different from the former); and, if any:

ii) telephone number and e-mail address.

b) egal entities:

i) registered office and main operational office (if different from the former);

ii) telephone number and e-mail address.

31. « *Money laundering* »:

a) the acts set forth in article 421-*bis* of the Criminal Code;

b) participation in one of the acts set forth in article 421-*bis* of the Criminal Code, association to commit such an acts, the attempt to perpetrate them, the fact of assisting, instigating or advising someone to commit them or the fact of facilitating their execution.

32. « *Close associates* »:

a) any natural person who has joint beneficial ownership of a legal entity or other close economic relationship with a person belonging to one of the categories established by sub-paragraphs 22 and 24;

b) any natural person who is the only beneficial owner of a legal entity de facto created for the benefit of a person belonging to one of the categories established by sub-paragraphs 22 and 24.

33. « *States at risk* »: States included in the lists published by international or regional bodies, or subject to enhanced monitoring mechanisms by international or regional bodies.

The Financial Information Authority provides the supervised entities with guidelines on the identification of the relevant international or regional bodies.

34. « *High-risk States* »: States with strategic deficiencies in their anti-money laundering and combating the financing of terrorism systems, included on the list published, and regularily updated, pursuant to the Instruction No. 1 on "High-risk States" of 23 October 2017 of the Financial Information Authority.

35. « *Beneficial owner* »: the natural person, in whose name and on whose behalf a relationship is opened or an operation or transaction is carried out, or, in the case of a legal entity, the natural person who, ultimately, owns or controls the legal entities in whose name in the name and on whose behalf a relationship is opened or an operation or transaction is carried out or that is beneficiary of it. In particular:

a) in case of legal entities, the beneficial owner is:

i) the natural person who ultimately owns or controls the legal entity, through ownership or control, direct or indirect, of a sufficient percentage of shares in the company's capital or voting rights, also through bearer negotiable shares;

ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s) or who exercise in other ways control on directing or managing the company; the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point i and this sub-paragraph ii);
b) in the case trust, the beneficial owner is:

i) the settlor;

ii) the trustee(s);

iii) the protector, if any:

iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;

c) in case of non profit entities, the beneficial owner is:

i) the natural person who effectively exercises control of the patrimony of the legal entity;

ii) if the future beneficiaries have already been established, the natural person who is the effective beneficiary of the patrimony of the legal entity;

iii) if the future beneficiaries of the legal entity have not yet been determined, the category of persons in whose principal interest the legal entity has been created or acts.

36. « *Transaction* »:

a) the transmission or movement of payment instruments;

b) a determined or determinable activity with an economic or financial objective, which modifies the existing juridical situation achieved by a professional performance.

37. « *Linked transaction* »: a transaction which, even if in itself autonomous, constitutes, from an economic perspective, a unique operation with one or more operations executed at different stages or moments.

38. « *Transfer of funds (or wire transfer)* »: a transaction carried out through electronic means by a payment services provider in the name of and on behalf of the one ordering with the purpose of placing funds at the disposal of a beneficiary in another payment services provider, even if the one ordering and the beneficiary are the same person.

39. « *Trust* »: a legal relationship established (*inter vivos* or *mortis causa*) by a person, the settlor, in which assets are placed under the control of a trustee in the interest of a beneficiary or for a specific purpose.

40. « *Customer* »: natural persons or legal entities *vis-à-vis* whom a supervised entity offers its services, according to its Statute, Regulation or internal policies.

Title II

Risk Based Approach

Article 4. *Risk based approach*.

1. Supervised entities shall modulate the intensity and extent of the due diligence obligations according to the level of risk of money laundering and financing of terrorism associated with the individual customer, or relationship, or operation or transaction, or transfer of funds, taking into account their own sectoral risk assessment.

2. Supervised entities shall exercise with autonomy and independence, and responsibility, an assessment of all the potentially significant risk factors relating to geographic area, the category of customer, the typology of relationships or service, operations or transaction or channel of distribution.

3. In view of assisting the assessment by supervised entities, the Financial Information Authority provides the risk factors included in the Annex 1, which are illustrative and not exhaustive.

Risk factors included in the Annex 1 are designed to mitigate the uncertainty margins associated with purely subjective or discretionary assessments and intend to promote the homogeneous fulfillment of the assessment and the consistent attribution of the risk profile to the customers.

4. Risk factors shall be considered in view of assessing the level or risk of money laundering and financing of terrorism, attributing a consistent risk profile to the customer, and associating a proportionate level of risk to relationships, operations or transactions, or transfer of funds. They do not necessarily constitute anomaly indicators for the purpose of suspicious activity reports.

Title III

Customers' Due Diligence

Chapter 1

Cases of application

Article 5. *Cases of application*.

1. Supervised entities shall carry out due diligence in the following cases:

a) when they establish a relationship;

b) when they carry out operations or transactions equal to or above euros 10,000, regardless of the fact that the operation or transaction is executed in a single operation or in several operations which appear to be linked;

c) when they make a transfer of funds equal to or above euros 1,000;

2. Supervised entities shall in any case fulfill the due diligence requirements:

a) where there is a suspicion of money-laundering or the financing of terrorism, regardless of any exemption or applicable threshold;

b) where there are doubts as to the reliability or adequacy of the data previously obtained for the identification of the customer, of persons delegated or in charge of operating in the name of, and on behalf of, the customer, or of the beneficial owner.

2. Pursuant to Article 5 (1), letter b), of the Law No. XVIII of 8 October 2013, the fulfillment of the due diligence requirements through third parties is forbidden.

Chapter 2

Object, Aims

Article 6. *Content, phases and purpose.*

1. Due diligence develops in two interconnected and interdependent phases, which have as their object:

a) *the identification*; and

b) *the verification of the identity*;

of the customers, of persons delegated or in charge of operating in the name of, and on behalf of, the customers, and the beneficial owners of the relationships or accounts, funds or other economic asset.

c) *obtaining and assessing the information relating to the nature and purpose of the relationship, or operation or transaction, or transfer of funds, and on the beneficial ownership and the origin of funds*.

2. The main purpose of the due diligence is the acquisition of the effective knowledge of the customers (*Know Your Customer*, KYC), the nature and purpose of the relationships, operations and transactions, or transfer of funds, and the attribution of a consistent profile to the customers.

Chapter 3

Periodicity and Requirements

Article 7. *Periodicity*.

1. The supervised entities shall carry out the due diligence:

a) prior to the opening a relationship, or prior to the carrying out an operation or transaction, or transfer of funds, in the cases indicated at Article 5;

b) in a constant manner, in the case of ongoing relationships.

2. The scope and periodicity of the due diligence measures may vary depending on whether the adoption of simplified, ordinary or enhanced due diligence is required.

Chapter 4

Ordinary due diligence

Section 1

Identification

Article 8. *Identification of the customer, and the delegated or persons in charge of operating, in the case the customer is a natural person*.

1. Supervised entities shall perform the identification, normally, with the presence of the customer.

2. Prior to the opening of a relationship, the operational functions shall identify the customer obtaining, *inter ali*a, the following document, data and information:

a) *identification data*:

b) *contact details*:

c) *copy of an identity document*;

d) *status e activity*.

3. When third parties are delegated of in charge of operating in the name of, and on behalf of, the customer, supervised entities shall obtain, *inter alia*, the following documents, data and information relating to each of them:

a) *identification data*;

b) *contact details*;

c) *copy of an identity document*;

d) *status e activity*;

e) *description of the relationhip with the customer and copy of the delegate or appointment*.

4. In the cases indicated at paragraph 3, the delegation or appointment become operational only after identification of the delegated or persons in charge of operating.

5. When doubts about the truthfulness of the information provided by the customer, or the authenticity of an identity document occur, supervised entity shall immediately contact the competent Authorities of the Holy See or of the State, in order to carry out the necessary checks.

6. In the cases indicated by paragraph 5, when the doubts remain, supervised entities shall file immediately a suspicious activity report to the Financial Information Authority.

Article 9. *Identification of the customer, of the delegated and the persons in charge of operating, in the case the customer is a legal entity*.

1. Supervised entities shall perform the identification, normally, with the presence of the natural person with the power of representation (representative) or the effective ownership (beneficial owner).

2. Prior to the opening a relationship, the operational functions shall identify the legal entity obtaining, inter alia, the following document, data and information:

a) copy of documents showing the nature and the proof of the existence of the legal entity;

b) copy of documents showing the governance bodies of the legal entity, including, inter alia, the names of the persons carrying out the functions of the management and senior management, and the beneficial owners;

c) description of the nature and purpose of the legal entity's activity;

i) in the case of non-profit entities, it must be indicated at least the categories of beneficiaries to whom the activities are destined and the geographic scope of the activities;

ii) in the case of entities such as foundations or legal arrangements, such as trusts, must be indicated the objectives pursued in practice, the beneficiaries and the trustee, as well as the management methods;

d) legal entity's identification data and contact details;

e) identification data and contact details of the natural person with the power of representation (representative) or the effective ownership (beneficial owner);

f) copy of an identity document of the natural person with the power of representation (representative) or the effective ownership (beneficial owner).

3. When third parties are delegated of in charge of operating in the name of, and on behalf of, the customer, supervised entities shall obtain, inter alia, the following documents, data and information relating to each of them:

a) *identification data*;

b) *contact details*;

c) *copy of an identity document*;

d) *status and activity*;

e) *description of the relationship with the customer and copy of the delegate or appointment*.

4. In the cases indicated at paragraph 3, the delegation or appointment become operational only after identification of the delegated or persons in charge of operating.

5. When doubts about the truthfulness of the information provided by the customer, or the authenticity of an identity document occur, supervised entity shall immediately contact the competent Authorities of the Holy See or of the State, in order to carry out the necessary checks.

6. In the cases indicated by paragraph 5, when the doubts remain, supervised entities shall file immediately a suspicious activity report to the Financial Information Authority.

Section 2

Nature and purpose of the relationship, and origin of funds

Article 10. *Obtaining and assessment of information relating to the nature and purpose of the relationship and on the origin of funds*.

1. Supervised entities shall acquire and assess information on the nature and purpose of the relationship.

2. The depth and extent of the acquisition and the assessment of the information indicated at paragraph 1 must be proportionate to the category and *status* of the customer, on the basis of a risk bases approach.

3. The operational functions shall obtain, inter alia, the following information:

a) *purpose of the opening of the relationship*;

b) *origin of the funds*;

c) *typology of services requested*;

d) *expected operations, including the potential volumes, economic reasons and counterparts*;

e) *where possible, customer's economic and financial situation, including the main sources of income or revenue*;

4. Part of the information on the nature and purpose of the relationship can be also deduced from the category and *status* of the customer, and from same typology of the relationship or the services requested by the customer, on the basis of a risk based approach.

Section 3

Verification of the identity

Article 11. *Verification of the identity of the customer, the delegated or person in charge of operating, or the beneficial owner in the case the customer is a legal entity.*

1. Prior to the opening of a relationship, the operational functions shall verify the identity of the customer, the delegated or person in charge of operating, and the beneficial owner in the case the customer is a legal entity, through the access of reliable sources, including, *inter alia*:

a) *Sources of the Holy See, the State and the Catholic Church*:

i) *Acta Apostolicae Sedis*;

ii) Pontifical Yearbook;

iii) Bulletin of the Holy See Press Office;

iv) Registers held by the Governorate of the Vatican City State;

v) Yearbooks or other official sources of Episcopal Conferences;

vi) Repertoire of the International Associations of the Faithful held by the Dicastery for the Laity, the Family and Life;

vii) Registers, records and lists made available by the competent foreign public Authorities.

b) Other reliable and independent sources and data bases.

Article 12. *Validation*.

1. Supervised entities shall adopt adequate procedures and measures for the validation of the identification and the verification of the identity of the customer, ensuring that:

a) the operational functions are endowed with internal procedures and manual, and carries out the validation for each due diligence procedure on a daily basis;

b) the control functions are endowed with internal procedures and manual and carries out the control of the validations carried out by the operational functions, on a quarterly basis, even with sample tests.

2. The validation must always be carried out by the control functions in the case of high-risk customers.

3. The control functions may have in any case a timely access to all documents, data and information obtained by the operational functions.

Section 4

Customer profile

Article 15. *Customer profile*.

1. All documents, data and information obtained pursuant to Articles 8-11 shall be registered in the personal customer form, to whom a consistent profile shall be attributed, including the following three elements:

a) category and *status*;

b) economic profile;

c) risk profile.

2. Operations and transactions carried out in the name of, and on behalf of, the customer, shall be consistent with the customer profile.

Article 14. *Risk profile*.

1. Operational functions shall attribute a risk profile to the customer on the basis of a comprehensive assessment of the documents, data and information acquired to the end of the due diligence, taking into account the related risk factors.

2. Supervised entities may automatically attribute a risk profile to the customer, through information and technology (IT) systems.

These systems shall allow, the overall assessment of the elements obtained pursuant to Articles 8-11, and ensure, inter alia, that:

a) weighting is not unduly influenced by one only factor;

b) weighting is not distorted by the consideration of too general categories;

c) weighting does not lead to a situation where it is impossible to classify a relationship as high risk or such that the majority of relationships are classified as high risk;

d) risk scores generated automatically by information and technology (IT) systems may be corrected, where necessary.

3. Supervised entities shall in any case ensure that the attribution of the risk profile is consistent with a risk based approach and with the customer's effective knowledge, and allow the fulfillment of the obligations established by the Law No. XVIII of 8 October 2013 and of this Regulation on high risk situations.

Article 15. *Validation*.

1. Supervised entities shall adopt adequate procedures and measures for the validation of the attribution of the risk profile to the customer carried out by the operational functions, ensuring that;

a) the operational functions are endowed with internal procedures and manual and carries out the validation for each due diligence procedure on a daily basis;

b) the control functions are endowed with internal procedures and manual and carries out the control of the validations carried out by the operational functions, on a quarterly basis, even with sample tests.

2. The validation must always be carried out by the control functions in the case of high-risk customers.

3. The control functions may have in any case a timely access to all documents, data and information obtained by the operational functions.

Article 16. *Update and change of the risk profile*.

1. Supervised entities shall define the ordinary frequency of updating the risk profile of the customer, consistently with the risk based approach and the level of risk associated to the customer.

2. Supervised entities shall in any case immediately update the risk profile of the customer upon the occurrence of triggering events, on the basis of the risk based approach.

3. The lowering of the risk profile of the customer shall be limited to exceptional cases, approved by control functions, and adequately motivated in written.

Section 5

Ongoing Customer Due Diligence

Article 17. *Ongoing customer due diligence*.

1. Supervised entities shall carry out an ongoing customer due diligence during the course of the relationship, in order to keep the customer profile updated and to identify potential anomaly indicators.

2. For the purposes of paragraph 1, supervised entities shall adopt adequate procedures and measures allowing to:

a) constantly monitor the relationship, including scrutinizing operations or transactions undertaken throughout the course of that relationship, so as to ensure that they are consistent the customer profile;

b) to keep updated documents, data and information acquired, consistently with the periodicity established by the policies indicated in Article 6, taking also into consideration the risk profile of the customer;

c) to keep updated the customer profile.

3. The updating of documents, data and information must be made, in any case, to the request for activation or termination of a service or a financial instrument.

4. Supervised entities shall adopt adequate policies, procedures and measures related to the dormant account.

Section 6

Due diligence in case of single operations or transactions, or transfer of funds

Article 18. *Single operations or transactions*.

1. In the case of operations or transactions equal to or above euros 10,000, regardless of the fact that the operation or transaction is executed in a single operation or in several operations which appear to be linked, supervised entities shall carry out the due diligence pursuant to Articles 8-11, unless, where the customer is the owner of a relationship:

a) the personal customer form is updated;

b) the operation or transaction is consistent with the customer profile;

c) no anomaly indicators are detected.

2. In the case of cross-border transportation of cash for an amount equal to or above euros 10,000, supervised entities shall not perform the operation or transaction before the user presents a copy or fill out the declaration of cross-border transportation of cash pursuant to Title VI of Law No. XVIII of 8 October 2013.

Article 19. *Transfer of funds*.

1. In case of transfer of funds equal to of above euros 1,000, supervised entities shall carry out the due diligence pursuant to Articles 8-11, unless, where the customer is the owner of a relationship:

a) the persona customer form is updated;

b) the operation or transaction is consistent with the customer profile;

c) no anomaly indicators are detected.

2. The transfer of funds must in any case be accompanied by data and information indicated in Title II of Regulation No. 2 of 12 December 2017.

Section 7

Remote Due Diligence

Article 20. *Remote identification*.

1. Without prejudice to the obligation of identification in the presence of the customer, in accordance with Articles 8 (1) and 9 (1), in case of remote request of a new relationship or operations or transactions the, the obligation of identification shall be deemed completed, even without the physical presence of the customer, in the cases indicated at paragraphs 2-5.

2. In the case of request for a new relationship by a subject belonging to one of the categories of customer authorized to access the services provided by the supervised entity, the identification shall be deemed completed when:

a) the identification data result from declaration or statement by the competent Authorities of the State of belonging or of the pontifical representative to the State where the customer is located;

b) the category and *status* of the customer are confirmed, where necessary, by the competent authority of the particular Church to which they belong;

c) the identification data result from public deeds, or authenticated private deeds, or qualified certificates used for the generation of a digital signature associated with information and technology (IT) documents, in the cases established by the legislation of the State;

d) possess a digital identity with a maximum level of security, as well as a digital identity with a maximum level of security or a certificate for the generation of a digital signature, issued under an electronic identification scheme, in the cases established by the legislation of the State;

3. In the case of a request by a customer for operations or transactions equal or above euros 10,000, the identification shell be deemed completed when:

a) the request from the user is acquired:

i) by fax or ordinary mail, with legible signature, attaching a copy of an identity document;

ii) by ordinary electronic mail (*e-mail*), attaching a copy of a document of identity;

iii) by maximum security electronic mail (*secure e-mail*);

b) the acquired data are verified in an appropriate manner, considering the user profile and the transmission methods used by the user, based on a risk-based approach;

c) there are no doubts about the coincidence between the customer to be identified and the subject to whom the documents, data and information acquired refer to;

d) the personal customer form is updated;

e) the operations or transactions requested are consistent with the customer profile;

4. In the case of a request by a customer for transfer of funds equal to or above euros 1,000, beside the cases where the communications channels established at paragraph 3, letter a), are used, taking into account what indicated at letters b)-e), the identification shall be deemed completed when strong customer authentication mechanisms established by Chapter 5 of the Regulation No. 3 of 23 May 2018, are used, such as the security token.

5. The remote identification in the cases indicated in paragraphs 2-4 shall be deemed completed even when it is carried out digitally remotely using audio/video tools according to the procedures set out in Annex 4.

6. The remote identification of the customer does not exempt:

a) from the verification of the identity, pursuant to Article 11;

b) from the validation, pursuant to Articles 12 and 15;

unless the supervised entity is authorized to carry out remote financial services on a professional basis, and the means of communication used by the customer allow direct access to financial services in digital form (on-line).

Chapter 5

Simplified Due Diligence

Article 21. *Cases of application.*

1. Supervised entities may apply simplified customer due diligence measures in the following cases:

a) cases of low level of risk indicated in Annex 2, and in particular:

i) is an organ or entity of the Holy See, indicated in the *Apostolic Constitution "Pastor Bonus" on the Roman Curia* of 28 June 1988 and subsequent amendments and in the Acts creating new organs and entities of the Holy See issued by the Supreme Pontiff;

ii) is an organ or entity of the State, indicated in the "*Fundamental Law of the Vatican City State*" of 22 February 2001 and in the Law no. CCCLXXXIV of 16 July 2002 on "*The Government of the Vatican City State",* and subsequent amendments;

iii) is a Vatican citizen resident in the Vatican City State.

iv) is a legal entity registered in the registries of the canonical legal persons or of the civil legal persons maintained by the Governorate of the Vatican City State;

v) is an employees or retirees of an organ or entity of the Holy See or the State indicated at subparagraphs i) and ii), unless the subject performs or performed additional working, professional or productive activities;

b) cases where the risk level attributed in line with Article 14 is low.

2. Simplified customer due diligence shall not apply, in any case:

a) cases where the enhanced due diligence shall be applied, pursuant to Article 24;

b) cases where the risk level attributed in line with Article 14 is high.

3. In the case of application of simplified due diligence measures, supervised entities shall ensure the attribution and updating of a consistent profile to the customer, and that the measures adopted allow to identify any factor that may require a potential increase in the level of risk and the implementation of the ordinary or enhanced due diligence.

4. Supervised entities shall communicate, on an annual basis, the typology of simplified due diligence measures adopted, including the aggregated data by category of customers, to the Financial Information Authority, which may request their revision.

Article 22. *Simplified requirements*.

1. In the cases established in Article 21, supervised entities may implement simplified measures in the phases of identification and verification of the identity of the customer, and the acquisition and assessment of information relating to the nature and purpose of the relationship and the origin of the funds, or of the operation or transaction, or the transfer of funds.

2. The operational functions, on the basis of a risk based approach, may implement, inter alia, the following simplified due diligence measures

a) in the phase of identification of the customer, the quantity of the requested information may be lower:

i) the information on the category and status, and activity, referred to in Article 8 (2) (d), in the case of an employee or retiree of the Holy See or the State, may be deducted from the typology of employment relationship, current or previous, unless the subject performs or performed additional working, professional or productive activities;

ii) the copy of the documents showing the nature and the proof of the existence of the legal entity, in accordance with Article 9 (2) (a), in the case of a legal person registered in the State, may be acquired by accessing the registers kept by the Governorate of the Vatican City State;

b) in the phase of obtaining and assessment of information on the nature and purpose of the relationship and on the origin of the funds, some information may be deducted from other accessible information:

i) the purpose of the relationship, the origin of funds, the typology of services requested, the expected operations, including the potential volumes, economic reasons and counterparts, as well as the customer's economic and financial situation, including the main sources of income of revenue, pursuant to Article 10 (3), in the case of an employee or retiree of the Holy See or the State, can be deduced from the typology of work relationship, current or previous, unless the subject performs or performed additional working, professional or productive activities;

c) in the phase of ongoing due diligence, the frequency and depth of the monitoring activities may be lower:

i) the monitoring of the relationship, the updating of documents, data and information, and of the customer's profile, referred to in Article 17 (2), may be less frequent than the ordinary due diligence;

ii) the monitoring of operations or transactions, may be carried out in the case they exceed predetermined thresholds.

3. The simplified due diligence measures referred to in paragraph 2 are without prejudice to the obligations to verify the customer identity and validation procedures.

Chapter 6

Enhanced Due Diligence

Article 23. *Cases of application.*

1. Supervised entities shall apply the enhanced due diligence measures in case one of the following situations occurs:

a) cases of high level of risk indicated in Annex 3, and in particular,

i) in the case the customer, or the beneficial owner pursuant to Article 3 (35), is a politically exposed person, or a family member, or a close associate, of a politically exposed person;

ii) in case of relationships, operations and transactions with natural persons or legal entities, including financial institutions, directly or indirectly connected to States at risk or High-risk States;

iii) in case of operations or transactions unusual or inconsistent with the profile of the customer, including unnecessarily complex or illogic schemes, operations or transactions;

b) cases where the risk level attributed in line with Article 14 is high.

2. Enhanced due diligence measures shall not substitute the ordinary due diligence measures, but they must be applied in addition to ordinary due diligence measures.

3. Supervised entities shall communicate, on an annual basis, the typology of enhanced due diligence measures adopted, including the aggregated data by category of customers, to the Financial Information Authority, which may request their revision.

Article 24. *Enhanced requirements*.

1. In the cases established in Article 23, supervised entities shall implement enhanced due diligence measures in the phases of identification and verification of the identity of the customer, and the acquisition and assessment of information relating to the nature and purpose of the relationship and the origin of the funds, or of the operation or transaction, or the transfer of funds.

2. The operational functions, on the basis of a risk based approach, shall implement, inter alia, the following enhanced due diligence measures:

a) in the phase of identification of the customer, the quantity of the requested information shall be greater in relation to:

i) the *status* and activity of the customer and the delegated or persons in charge of operating, in the case the customer is a natural person, pursuant to Article 8 (2) (d) (3) (d);

ii) the nature and purpose of the legal entity's activity, and on the *status* and activity of the delegated or in charge of operating, in the case of customer is a legal entity, pursuant to Article 9 (2) (c);

iii) the *status* and activity of the natural endowed with the beneficial ownership of the legal entity (beneficial owner), pursuant to Article 9 (2) (e);

b) in the phase of acquisition and assessment of information on the nature and purpose of the relationship and on the origin of the funds, the quantity of the requested information shall be higher in relation to:

i) the origin of the funds deposited or handled in the relationship, and where the funds come from a third party, information about the relationship between the customer and the originator of the funds, the reason of the transfer, as well as on the consistency between such transfer and the customer profile;

ii) expected operations, including the potential volumes, economic reasons and counterparts;

iii) economic and financial situation of family members and close associates, if the customer is a politically exposed person.

c) in the phase of ongoing due diligence, the frequency and depth of the monitoring activities shall be greater:

i) the monitoring of the relationship, referred to in Article 17 (2), shall be more frequent than the ordinary due diligence, and shall be in any case carried out at least once every six months, to the ends of detecting any factor influencing the risk profile of the customer;

ii) the monitoring and analysis of operations or transactions shall always be carried when the threshold exceeds a predetermined threshold, with shall be lower that established for the ordinary due diligence, on the basis of a risk based approach;

d) in case of operations or transactions unusual or inconsistent with the profile of the customer, including unnecessarily complex or illogic schemes, operations or transactions;

i) if there are no anomaly indicators that make it mandatory to file a suspicious activity report to the Financial Information Authority, further information shall be required on the economic reason of the operation or transaction, on the beneficial ownership, origin and destination of the funds.

3. The enhanced due diligence measures referred to in paragraph 2 are without prejudice to the obligations to verify the customer identity and validation procedures.

Chapter 7

Completion of the Due Diligence and Duty to Refrain

Article 25. *Completion of the due diligence and duty to refrain*.

1. Supervised entities shall complete the due diligence prior the establishing of the relationship or the execution of an operation or transaction, in the cases established in Article 5.

2. When it is not possible to complete the due diligence (either with the presence of the customer, or remotely), it is prohibited to open a relationship or to execute any operation or transaction.

3. When it is not possible to complete the ongoing due diligence, it is mandatory to close the relationship and prohibited to execute any operation or transaction.

4. In the cases indicated at paragraphs 2 and 3, supervised entities shall immediately file a suspicious activity report to the Financial Information Authority.

5. In the case of dormant accounts, in addition to the provision referred to paragraph 4, the supervised entities shall consider the specific anomaly indicators established by Regulation No. 5 of 19 September 2018 for the purpose of filing a suspicious activity report.

6. In the event of due diligence related to the suspicion of money laundering or financing of terrorism, pursuant to Article 5 (2), if the fulfillment of the identification and verification obligations may reveal such suspicion to the customer, or affect the pursue of the beneficiaries of the suspicious operation or transaction, or in general the activities of the competent Authorities, supervised entities may execute the operation or transaction and shall immediately file a suspicious activity report to the Financial Information Authority.

Title IV

Due diligence Obligations in the case of financial institutions

Article 26. *Requirements*.

1. Supervised entities shall adopt specific measures for the due diligence in case of relationship with foreign financial institutions.

2. The measures referred to at paragraph 1 include, *inter alia*:

a) obtaining sufficient information to adequately understand the nature and good standing of the foreign financial institution, as well as the supervisory regime to which it is subject;

b) verifying that the foreign financial institution is not a shell bank;

c) verifying the existence of adequate controls for the prevention and combating of money laundering and the financing of terrorism within the foreign financial institution;

3. Supervised entities shall also, *inter alia*:

a) obtaining the authorization by the senior management before opening correspondence accounts or establishing new relationships with foreign financial institutions;

b) establish in writing the burdens and responsibilities of their own and of the financial institutions with which they have relationships;

c) update at least on an annual basis the data and information about the foreign financial institutions with which they have relationships.

4. In the case of payable through accounts, supervised entities shall furthermore ensure that the foreign financial institution:

a) has carried out customer due diligence on the customers who have direct access to those accounts;

b) has fulfilled the requirements of customer due diligence, including adequate ongoing customer due diligence and, upon request, is able to supply promptly data and information obtained following the fulfilment of those requirements.

5. The provision referred to paragraph 4, letter b), is without prejudice of the provision referred to Article 5 (1), letter b), of the Law No. XVIII of 8 October 2013, forbidding the fulfillment of the due diligence requirements through third parties.

Title V

Registration and record-keeping

Article 27. *Registration and record-keeping*.

1. The supervised entities shall ensure the registration and record-keeping of all documents, data and information obtained to the ends of the due diligence for a period of ten years from the termination of the relationship or account, from the execution of an operation or transaction, pursuant to Article 38 of Law No. XVIII of 8 October 2013.

2. The documents, data and information to be registered and kept includes the information and documents that have been collected during the remote due diligence, including the customer's video-identification session and connected audio-video files, images and metadata in electronic format.

Title VI

Administrative Sanctions

Article 28. *Administrative sanctions*.

1. In case of violation or systematic non-fulfilment of the obligations established by this Regulation by supervised entities, the Financial Information Authority applies the administrative sanctions pursuant to Article 47 of Law No. XVIII of 8 October 2013.

Title VI

Final provisions

Article 29. *Final provisions.*

1. The provisions of this Regulation are without prejudice to the provisions of Regulation No. 5 of 19 September 2018 on "*Suspicious Activity Reports*" and of Instruction No. 1 of 23 October 2017 "*With which is published the list of high-risk States, with strategic deficiencies in their anti-money laundering and combating the financing of terrorism systems*", and subsequent amendments.

2. For matters not governed by this Regulation, reference should be made to the provisions of the law and regulations into force.

This Regulation enters into force the day of its publication on the official web site of the Financial Information Authority.

Vatican, 19 September 2018

RENÉ BRÜLHART
President

Visto

TOMMASO DI RUZZA
Director

Annex 1

Risk Factors

A. Risk factors associated to the geographic area.

Supervised entities shall consider the risk factors associated to the geographical area and the relationship between the customer and the geographic area.

1. Supervised entities shall identify the State or geographic area where the customer:

a) has the residence of domicile, or registered or operational offices;

b) mainly performs his activities;

c) mainly performs or receives transfers of funds;

d) has significant personal, institutional or professional connections.

Supervised entities shall determine the relative importance of individual State and geographical risk factors in accordance with the nature and purpose of the relationship.

2. In assessing the risk factors associated to individual State or geographical, supervised entities shall take into account, inter alia, the following elements:

a) *where the funds used in the relationship have been generated in a foreign State*: the effectiveness of the system for preventing and countering money laundering and financing of terrorism, and in particular the criteria for the identification of the predicate offence of money laundering;

b) *where the customer is resident or domiciled, or has the registered or operational office, in the case of a legal entity, in a foreign State*: the effectiveness of the system for preventing and countering tax offenses;

c) *where funds are received from, or sent to, States where groups committing terrorist offences are known to be operating*: to what extent this could be expected to or might give rise to suspicion, based on what the supervised entities know about the nature and nature of the relationship;

d) *in the case of correspondence account with foreign financial* institutions: the effectiveness of the supervisory and regulatory system;

Supervised entities shall in any case attribute a high level of risk to the States included in the list attached to Instruction No. 1.

B. Risk factors associated to the category of the customer.

Supervised entities shall consider the risk factors associated to the category of customer.

1. Supervised entities shall consider, inter alia, the risk associated to:

a) category and status of the customer;

b) economic profile of the customer;

c) activity of the customer;

d) behavior of the customer and its consistency with the nature and purpose of the relationship;

e) reputation of the customer.

2. Supervised entities shall monitor constantly the consistency between the products, services, operations or transactions performed or requested by the customer and his category and status, economic profile and activity, and behavior, updating consequently the risk profile of the customer.

B.1. Specific risk factors associated to the category of customer.

In assessing the risk factors associated to the category of the customer, supervised entities shall take into account, inter alia, the following elements:

a) in case of natural person:

i) whether the customer is a family member or a close associate to a politically exposed person;

ii) whether the customer holds a prominent position that might enable her to abuse of this position for private gain;

iii) whether the customer is not an employee or retiree of an organ or entity of the Holy See or the State;

iv) whether the customer, in addition to being an employee or retiree of an organ or entity of the Holy See or the State, performs or performed additional working, professional or productive activities;

v) whether the subjects delegated or in charge of operating in the name, and on behalf, of the customer, do not have links with the customer to justify the delegation or appointment;

b) in case of legal entity:

i) whether the customer has the registered or operational office in a high-risk State or a State at risk;

ii) whether the customer is not an entity of the Catholic Church;

iii) whether the customer is not registered in register held by the Governorate of the Vatican City State;

iv) whether the members of the management, or the senior management, or the beneficial owner, are politically exposed persons, or family members, close associates of politically exposed persons;

v) whether the member of the management, senior management, or the beneficial owners, might have a conflict of interest or abuse of their position for private gain.

vi) whether the governance model is unnecessarily complex or illogic or not transparent, without an apparent reason;

vii) whether changes having a negative impact in the control systems of the customer are registered;

viii) whether the delegated or in charge of operating in the name, and on behalf of, the customer, do not have a position in the organizational structure of the customer to justify the delegation or appointment.

ix) whether the customer could be for a fictitious ownership of funds or other assets;

B.2. Specific risk factors associated to the activity of the customer.

In assessing the risk factors associated to the activity of the customer, supervised entities shall take into account, inter alia, the following elements:

a) whether the customer does not carry out an activity of an institutional nature;

b) whether the customer performs or requests operations or transactions in high-risk sectors or with counterparts operating in high-risk sectors (for example, buying or selling metals or precious stones, or coins, or other values, real estate, trading goods or services in relation to cash operations), without an apparent reason.

c) if the customer performs or requests operations or transactions unnecessarily complex or illogic, of an unusually high amount, or characterized by anomalous patterns, without an apparent consistency with the nature and purpose of the relationship or the profile of the customer;

d) whether, over time, the activity of the customer is not consistent with the information collected by the supervised entity on: status and activity, purpose of the opening of the relationship, origin of the funds, typology of services requested, expected operations, including potential volumes, economic reasons and counterparties.

B.3. Specific risk factors associated to the behavior of the customer.

In assessing the risk factors associated to the behavior of the customer, supervised entities shall take into account, inter alia, the following elements:

a) whether the customer is not cooperative in the phase identification;

b) whether the customer is not able to provide the documents, data and information requested;

c) whether the customer requests unnecessary or unreasonable levels of confidentiality, or is reluctant to provide information on his activity;

d) whether the customer looks for out one or more operations or transactions where the establishment of a relationship might make more economic and operational sense;

B.4. Specific risk factors associated to the reputation and integrity of the customer.

In assessing the risk factors associated to the reputation of the customer, supervised entities shall take into account, inter alia, the following elements:

a) whether reliable and persistent adverse reports about the customer, or the members of the management, or the senior management or the beneficial owners, if a legal entity

b) whether reliable and systematic negative reports are registered on the honorability of the customer, or that of the members of the management, or the senior management or the beneficial owners, if a legal entity;

c) whether the supervised entity is aware of suspicious activity reports, inquiries or inspections, investigations or judiciary proceedings, involving the customer;

d) whether the customer, or the members of the management, or the senior management or the beneficial owners, if a legal entity, are subjects to preventive measures of a personal or real nature

C. Risk factors associated to the typology or relationship, product or service, operation or transaction.

1. In assessing the risk factors associated to the typology or relationship, product or service, operation or transaction, supervised entities shall take into account, inter alia, the following elements:

a) the level of transparency or opaqueness of the product or service, operation or transaction;

b) the complexity of the product or service, operation or transaction;

c) the value or size of the product or service, operation or transaction.

2. The following products or services, or factors, may contribute to reducing risk:

a) a product or service with limited functionality, such as, for example:

i) has fixed term with low savings thresholds;

ii) benefits cannot be realized in favor of a third party;

iii) benefits are only realizable in the long term or for a specific purpose (such as: pension funds);

iv) a low-value advances on salaries, including ones that are conditional on the purchase of a specific good or service;

b) a service based on the presence of a current account and which can only be used through the same current account.

3. The following products or services, or factors, may contribute to increasing risk:

a) a product or service that places no restrictions on amount, cross-border transactions or similar product features;

b) new products, including new channels of distribution, and the use of new or evolving technologies for new or pre-existing products, without adequate safeguards.

c) unusually large volume of the operations or transactions;

d) investment products managed discretionally by third parties.

C.1. Specific risk factors associated to the level of transparency or opaqueness or the product or service, operation or transaction.

In assessing the risk factors associated to the level of transparency or opaqueness or the product or service, operation or transaction, supervised entities shall take into account, inter alia, the following elements:

a) whether products or services, operations or transactions, allow the customer to remain anonymous, to hide the ownership, origin or destination of the funds;

b) whether a third party, that is not part of the relationship, has de facto the possibility to give instructions on the management of the relationship.

C.2. Specific risk factors associated to the complexity of the product or service, operation or transaction.

In assessing the risk factors associated to the complexity of the product or service, operation or transaction, supervised entities shall take into account, inter alia, the following elements:

a) whether the product or service allows transfers by, or in favor of, third parties, of a higher amount than what is normally expected for similar products or services;

b) whether the product or service is not listed on regulated markets.

c) whether the operation or transaction involves multiple subjects or States.

C.3. Specific risk factors associated to the value or size of the product or service, operation or transaction.

In assessing the risk factors associated to the value or size of the product or service, operation or transaction, supervised entities shall take into account, inter alia, the following elements:

a) whether the product or service facilitates or encourage high-value operations or transactions;

b) whether the transactions are higher than what is reasonable to expect considering the category and status, and activity, of the customer.

D. Risk factors associated to the channel of distribution.

In assessing the risk factors associated to the value or size of the product or service, operation or transaction, supervised entities shall take into account, inter alia, the following elements:

a) whether the relationship is managed exclusively on a non-face-to-face basis;

b) whether the management of the relationship by the supervised entity requires in all phases the presence of a foreign financial intermediaries.

Annex 2

Factors Indicating Potential Low Risk Situations

The following factors are considered as indicating a low risk situation.

A. Geographic area.

It is assumed that the following States are associated to a low level of risk.

a) Vatican City State;

b) States that impose obligations to prevent and counter money laundering and financing of terrorism equivalent to those established in the State, pursuant to Article 10 (2) (b) (ix) of Law No. XVIII of 8 October 2013.

B. Category of the customer.

It is assumed that the following categories of customers are associated to a low level of risk.

a) Organs or entities of the Holy See indicated in the Apostolic Constitution "Pastor Bonus" on the Roman Curia of 28 June 1988 and subsequent amendments and in the Acts creating new organs or entities of the Holy See issued by the Supreme Pontiff;

b) Organs or entities of the State indicated in the "*Fundamental Law of the Vatican City State*" of 22 February 2001 and in the Law no. CCCLXXXIV of 16 July 2002 on the "*The Government of the Vatican City State*", and subsequent amendments;

c) Vatican citizens residents in the Vatican City State.

d) Legal entities registered in the registries of the canonical legal persons or of the civil legal persons maintained by the Governorate of the Vatican City State;

e) Employees or retirees of organs or entities of the Holy See or the State indicated at letters a) and b), unless the subject performs or performed additional working, professional or productive activities.

C. Typology of relationship, product or service, operation or transaction or channels of distribution.

It is assumed that the following relationship, product or service, operation or transaction or channels of distribution. are associated to a low level of risk.

a) Relationships whose main purpose is the crediting of salary or pension and organ or entity of the Holy See or the State.

b) Pension or similar scheme that provides retirement benefits to employees, where the scheme rules do not permit the assignment of a member's interest under the scheme.

c) Advance funds connected to a relationship whose beneficial owner is s subject to whom a low level of risk is associated.

d) Individual wealth managements linked to a relationship.

e) Custody and management of portfolio linked to a relationship.

f) Cashier’s checks connected to a relationship whose beneficial owner is s subject to whom a low level of risk is associated.

Annex 3

Factors Indicating Potential High Risk Situations

The following factors are considered as indicating a high risk situation.

A. Geographic area.

It is assumed that the following States are associated to a high level of risk.

a) High-risk states included in the Instruction No. 1 "*With which is published the list of high-risk States, with strategic deficiencies in their anti-money laundering and combating the financing of terrorism systems*" of 23 October 2017, and subsequent amendments;

b) States included in the lists published by international or regional bodies, or subject to enhanced monitoring mechanisms by international or regional bodies.

B. Category of customer.

It is assumed that the following categories of customers are associated to a high level of risk.

a) Natural person residents or domiciled, legal entity with registered office or operational offices in a high risk State or in a State at risk.

b) Subjects included in the list of subjects threatening international peace and security, issued by the President of the Governorate of the Vatican City State, as well as in the lists of designated subjects issued by the competent organs of the Security Council of the United Nations and of the European Union;

c) Politically Exposed Persons, their family members, or close associates.

d) Subjects not included in the categories of customers authorized to access services provided by the supervised entity receiving a relationship or account by succession or donation.

C. Typology of relationship, product or service, operation or transaction or channels of distribution.

It is assumed that the following relationship, product or service, operation or transaction or channels of distribution. are associated to a high level of risk.

a) Relationships characterized by anomalous profiles or kept with anomalous modes.

b) Relationships managed exclusively on a non-face-to-face basis, without adequate safeguards.

c) Relationships with delegated, or persons in charge of operating, with no apparent link with the customer.

d) Relationships with operations, including incoming or outgoing payments, not justified by the nature and purpose of the relationship or the profile of the customer.

e) collections of payments received from third party with no apparent link with the customer.

f) Schemes, operations or transactions characterized by a significant use of cash, without an apparent reason.

g) New products, including new channels of distribution, and the use of new or evolving technologies for new or pre-existing products, without adequate safeguards.

Annex 4

Video-identification procedure in case of remote due diligence

1. Supervised entities may fulfill the remote due diligence through the video-identification.

2. Supervised entities shall adopt systems ensuring the encryption of the audio/video communication channel through standardized mechanisms, applications and protocols updated to the latest version, as well as the maximum functionality and accessibility by the customers.

3. Supervised entities shall ensure that the video-identification complies with the following technical requirements:

a) the video images must be in color and allow clear visualization the interlocutor in terms of brightness, sharpness, contrast, fluidity of the images;

b) the audio must be clearly audible, without noticeable distortions or disturbances;

c) the audio/video session, which relates to the video images and the audio of the customer e of the operator, must be carried out in environments without particular disturbing elements.

4. Supervised entities shall ensure that the operator responsible for the activity refrains from starting the identification process or suspend it if the quality of the audio/video communication channel is particularly poor or retained not adequate to allow customer identification.

5. Supervised entities shall adopt adequate video identification procedures, which includes, *inter alia* the following phases:

a) the operator of the supervised entity ("operator") declares his name and surname, and function;

b) the operator obtains the consent to audio/video recording and its conservation and informs that the audio/video recording will be stored in a secured mode;

c) the customer confirms the identification data and contact details as defined at Articles 3 (9) and 3 (30) of this Regulation;

d) the customer confirms the willingness to open a relationship or perform an operation or transaction, indicated in the communication to the supervised entity, to which a copy of the identity document is attached;

e) the operator asks the customer expose the identity document (front and back) to the recording device, making possible the display of the photograph of the holder and the reading of the information contained in it (place and date of birth, number of document, issue and expiry date, issuing authority);

f) where necessary, the operator verifies the category, status and activity of the customer, especially in the case of doubts about the consistency between the customer's request and profile;

g) in case of negative result of the video-identification session, for any reason (for example, the identity document does not have the characteristics indicated in Article 3 (12) of this Regulation; or doubts persists about the customer's category, status and activity; or an inconsistency between the customer's request and profile is detected; etc.) the operator can exclude the admissibility of the remote due diligence;

h) in the case of positive result of the video-identification session, the operator sends to the customer:

i) summarizes the willingness expressed by the customer to open a relationship or perform an operation or transaction, collecting the confirmation from the same customer.

ii) a short text message (SMS) at the mobile's number declared by the customer, that the same customer is required to expose to the recording device;

iii) an e-mail to the e-mail address declared by the customer, with a link to a universal resource locator (URL) specially prepared for verification.

6. The audio/video session is fully recorded and adequately stored pursuant to Article 27 of the present Regulation.