Opinion No 1/2018
of the Financial Market Supervision Unit of Národná banka Slovenska
of 10 December 2018,
on the identification and verification of natural person clients not physically present by technical means and procedures in accordance with the Act on the prevention of money laundering and terrorist financing

The Financial Market Supervision Unit of Národná banka Slovenska (NBS), based on the provisions of Article 1(3)(a) point 3 of Act No 747/2004 Coll. on financial market supervision (and amending certain laws), as amended, after consultation with the Financial Intelligence Unit of the Police Force Presidium's National Crime Unit has issued this Opinion:

Article 1
Basic provisions

1. Under the provisions of the Act effective from 15 March 2018, obliged entities may identify and verify a natural person client using technical means and procedures[1] (hereinafter the "technology") without the client being physically present.

2. Before starting to use such technology, an entity which is a supervised entity or an entity applying for authorisation to perform activities under the supervision of Národná banka Slovenska or registration under a separate law[2] (hereinafter jointly a "supervised entity") must assess whether identification and verification of a natural person client using such technology without the client being physically present can be performed with a level of credibility equal to verification in their physical presence. In identification and verification, a supervised entity must take account of the circumstances of the execution of a transaction and the security risks of the technical means used.

3. This opinion aims to provide clarification for supervised entities concerning Národná banka Slovenska's general views on technologies used for identification and verification of natural person clients without the client being physically present in the performance of customer due diligence in supervised entities under a separate law.[3] This opinion does not apply to identification and verification in the provision of payment services under a separate regulation.[4]

4. For the purposes of this opinion:
   (a) **Technical means** are means for identification and verification of a natural person client, in particular a software solution of the supervised entity defined by a secure digital interface enabling the retrieval and transmission of data, documents and information through technical equipment and their subsequent processing, based on

[1] Article 8(1)(a) of Act No 297/2008 Coll. on the prevention of money laundering and terrorist financing (and amending certain laws).
[2] Act No 483/2001 Coll. on banks (and amending certain laws), as amended; Act No 492/2009 Coll. on payment services (and amending certain laws), as amended; and Act No 129/2010 Coll. on consumer credits and on other credits and loans for consumers (and amending certain laws), as amended.
[3] Act No 297/2008 Coll. on the prevention of money laundering and terrorist financing (and amending certain laws), as amended.
[4] Article 2(1)(g) and (h) of Act No 492/2009 Coll. on payment services (and amending certain laws), as amended.

which the supervised entity performs identification and verification of the natural person client without the client being physically present with a level of credibility equal to verification in their physical presence;

(b) **Procedure** is a purposeful and fixed sequence of linked steps in the identification and verification of a natural person client;

(c) **Sensitive data** is data, particularly personal data under a separate law,[5] which is used in the identification and verification of the natural person client.

Article 2
Obligations in implementation of a new method for identification and verification of a natural person client without the client being physically present

1. When considering the risk factor in terms of product, service, business, distribution channel and geography, the supervised entity should ensure that identification and verification of a natural person client without the client being physically present is used only for such products and services which are, with reference to their nature and extent, adequate and appropriate for this method of client verification.

2. When considering the risks, the supervised entity should assess the client's risk category, the client's behaviour during the use of technical means and any relevant risk factors, in particular the factors listed in Annex No 2 of the Act.[3] Upon request of Národná banka Slovenska, the supervised entity should be able to demonstrate how it identified, assessed and mitigated the individual risk factors. The supervised entity should take measures to ensure that the person responsible for the execution of tasks in anti-money laundering/countering terrorist financing (AML/CFT) is involved in the process of implementing any new method for identification and verification of the client without the client being physically present.

3. Prior to deciding on the use of technology from an external supplier, the supervised entity should assess and evaluate, in addition to the risks associated with the technical means, also other risks such as the suitability of the supplier of technical means, the duration of its operation on the market, customer references and the overall reputation of the supplier on the market, as well as the results of tests of the technical means.

4. The competent management body that approves the technology for the identification and verification of a natural person client without the client being physically present should bear responsibility for its implementation.

5. The method of evaluating and managing risks related to the identification and verification of a natural person client without the client being physically present, should be included in the Programme of internal activities under Article 20(2)(c) of the Act.[3]

6. The supervised entity should incorporate training on the practical use of the technical means and on how to identify potentially suspicious transactions related to the use of the technical means into the content and timetable of training of the staff who may encounter an unusual

[5] Article 2 of Act No 18/2018 Coll. on the protection of personal data (and amending certain laws).

transaction in their work. The training should be a part of regular education in the field of AML/CFT.

7. The control mechanism for the implementation and proper functioning of the technology should be in line with acts of general application[6] and consider the applicable risk management procedures.

8. The correctness, quality and operational safety of the technical means should be tested regularly. In addition, the supervised entity should continuously monitor the evaluation of effectiveness, safety and proper functioning of the technical means. Any detected errors, deficiencies or vulnerabilities of the technology should be removed by the supervised entity without delay after their identification and in the event of serious findings, the use of the technical means should be suspended until they are removed.

9. The supervised entity should introduce an update procedure for the technical means including a procedure for repairing the technical means in case of security problems and other errors and incidents. To this purpose, the supervised entity should take measures which allow the making of necessary change or the introduction of a new technology.

10. The supervised entity should have a plan in place that ensures continuity of its provided services and related activities if the technical means fail and are not able to fully ensure the required quality of identification and verification of a natural person client without the client being physically present. The supervised entity should test its continuity plan at regular intervals.

11. Prior to implementation of the identification and verification through technology of a natural person client without the client being physically present, the supervised entity should comply with the obligation to notify Národná banka Slovenska in accordance with applicable legal regulations.[7]

Article 3
Technology security

1. The technology should include a sequence of specific steps and logical links between individual system components to obtain the data, information and documents needed for the identification and verification of the natural person client and for their transfer, processing and evaluation.

2. The technical means should comply with technical standards for system security and systems for accessing sensitive data (such as encryption, validation of keys and certificates, signing of reports, technical and organisational arrangements for sensitive data, etc.) and

[6] For example, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Act No 18/2018 Coll. on the protection of personal data (and amending certain laws).

[7] Article 9(4) of Act No 483/2001 Coll. on banks (and amending certain laws), as amended; Article 65(4) of Act No 492/2009 Coll. on payment services (and amending certain laws), as amended; Article 20(6) of Act No 129/2010 Coll. on consumer credits and on other credits and loans for consumers (and amending certain laws), as amended, in conjunction with Article 20 of Act No 297/2008 Coll. on the prevention of money laundering and terrorist financing (and amending certain laws).

must comply in particular with the GDPR[8] and the Personal Data Protection Act,[9] and they must also be able to ensure the integrity of sensitive data and their protection against unauthorised access, change, loss and leakage.

Article 4
Technology features

1. The technical means should verify the authenticity, accuracy and completeness of data, documents and information related to the identified natural person in a way comparable to procedures in the person's physical presence. The procedures should include verification of identification from the supervised entity's internal sources (for example in the case of existing clients) or from independent external sources (such as records of identity documents and data stated in identity documents, lists of politically exposed persons and sanctioned persons in trusted third-party databases) or a combination of the above sources.

2. In identification and verification of a natural person client without the client being physically present, the supervised entity must specifically ensure that the technical means have the following functions:
   (a) Acquisition of authentic biometric data[10] or other comparable data in identification of the natural person client, and the trusted verification of such data;
   (b) Detection of discrepancies in authentic biometric data or other comparable data during data transfer in identification of the natural person client, and settings for compliance parameters;
   (c) Verification of obtained biometric data or other comparable data from internal or external sources or a combination thereof;
   (d) Authentic biometric data or other comparable data obtained for identification and verification of the natural person client are comparable/equivalent to the means used in identification and verification of a natural person client in their physical presence;
   (e) Acquisition of other personal data of an identified natural person client besides those referred to under (a) (for example, an identity document);
   (f) Verification of the authenticity and currency of other personal data obtained in addition to those referred to under (a) (for example, to compare an identity document with data from internal or external sources or a combination thereof, including verification of the security features of the identity document);
   (g) Detection of non-standard or risky features in the situation or the behaviour of an identified natural person client in non-verbal or verbal communication or in monitoring of the supervised entity with an identified client.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[9] Act No 18/2018 Coll. on the protection of personal data (and amending certain laws).
[10] Article 5(c) of Act No 18/2018 Coll. on the protection of personal data (and amending certain laws).

Article 5
Final provision

This opinion enters into force on the day of its approval by the Director of the Financial Market Supervision Unit of Národná banka Slovenska.

Done at Bratislava on 13 December 2018.

Ing. Vladimír Dvořáček
Member of the Bank Board and Executive Director
of the Financial Market Supervision Unit