NON-FACE-TO-FACE IDENTIFICATION METHODS IN CUSTOMER DUE DILIGENCE AND VERIFICATION OF IDENTITY

Non-face-to-face identification

The need for digital non-face-to-face identification has been growing for some time now, as services are provided digitally both domestically and across borders. The current maintenance of social distancing is likely to further accelerate the trend.

In a non-face-to-face identification situation, the customer is not physically present at the commencement of a customer relationship or in connection with the execution of a transaction. The obliged entity accordingly identifies the customer by obtaining customer due diligence data and verify the customer's identity using a non-face-to-face identification method or methods of its choice.

Risk-based approach

In a risk-based approach, obliged entities create their own customer due diligence procedures and the minimum criteria they will follow in their customer relationships. When assessing risk related to non-face-to-face identification, the obliged entity must pay particular attention to the nature of its own operations and the riskiness of its field of business as well as the scope of operations and the geographical location of customers. Based on a risk assessment, the obliged entity must assess which additional enhanced due diligence measures related to non-face-to-face identification, as provided for in the Money Laundering Act, are necessary for the obliged entity to be able to reduce the potentially higher risk of money laundering and terrorist financing associated with non-face-to-face identification.

Enhanced due diligence obligation associated with non-face-to-face identification

If the customer is not physically present for identification and identity verification (non-face-to-face identification), the party subject to the reporting obligation shall take the following measures to mitigate the risk of money laundering and terrorist financing:

- verify the customer's identity on the basis of additional documents or information obtained from a reliable source
- ensure that the payment of the transaction is made from the credit institution's account or to an account that was opened earlier in the customer's name
- verify the customer's identity with a means of identification as referred to in the Identification Act[1] or with a qualified certificate for electronic signature[2] or with some other electronic identification technology that is secure and verifiable.

In non-face-to-face identification situations, reliable customer identification and verification of identity may require a combination of different methods as well as requests for additional information from the customer and from reliable sources, particularly in the case of cross-border service provision and

[1] Act on Strong Electronic Identification and Electronic Trust Services (617/2009)

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

customer relationships initiated with a customer in another country. It is the responsibility of the obliged entity to assess the necessary additional measures for enhanced customer due diligence.

Non-face-to-face identification methods

At the establishment stage of a customer relationship, the customer is remotely identified, and their identity verified using some non-face-to-face identification method or a combination of several methods. The obliged entity must have in place methods with which to check the information provided by the customer through non-face-to-face identification. The information provided by the customer can be checked using information obtained from public registers classified as reliable sources. Such registers include, for example

- registers maintained by the Finnish Patent and Registration Office, such the Trade Register and the Register of Associations
- the Population Register, maintained by Digital and Population Data Services Agency
- the credit data register maintained by Suomen Asiakastieto Oy[3].

The obliged entity should note that information from corresponding public registers is not always available in other countries. If information is available, the obliged entity must assess the timeliness, reliability and accessibility of the information obtained from the foreign register. In addition to reports received from reliable sources, social media identifiers provided by a private service provider, email address, telephone number and a service in which another service provider has already identified the customer, for example using credit card information, may be utilised in customer due diligence, based on the obliged entity's risk assessment.

Means of strong electronic identification under the Identification Act

The Finnish Communications Regulatory Authority (Traficom) supervises compliance with the Identification Act[4]. Strong electronic identification services currently available include

- online banking codes of banks
- mobile certificates of telecommunications operators
- Population Register Centre citizen certificate on an identity card granted by the police
- certain other identification certificates
- identification broker services registered on various organisation cards.

Precise requirements are laid down for means of strong electronic identification, such as an obligation to submit a notification to Traficom prior to commencing a service, an audit obligation and an obligation to notify disruptions. Traficom maintains a list of identification services that meet the requirements of the law.[5]

[3] For the purposes under the Credit Information Act (527/2007).
[4] Act on Strong Electronic Identification and Electronic Trust Services (617/2009)
[5] https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification

Other electronic identification technology

With the development of technology, it is possible in non-face-to-face identification solutions to utilise, for example, artificial intelligence as well as blockchain technology, which enables new ways of building services and storing data. In customer non-face-to-face identification, information obtained from different data sources should be utilised by comparing and combining it with the information provided by the customer and information obtained via reliable sources.

Artificial intelligence is currently being used, at least in facial recognition and in verifying the authenticity of physical identity papers. In digital initial identification[6], customers can verify themselves with a mobile device, a passport (or some other proof of identity) and their own face. There are applications on the market that verify the authenticity of proofs of identity by checking security features, such as the authenticity of holograms. With biometric passports, the application is able to read the passport chip. The application verifies the customer's face from the face image taken by the customer, and a moving image verifies that the customer is alive.

Transparency of non-face-to-face identification process and storage of identification data

Non-face-to-face identification must be transparent (secure and verifiable) and it must be possible to review it later. Customer data must be stored in accordance with the retention period provided for in the Money Laundering Act, taking into account data protection and data security (confidentiality, integrity and availability). The person being identified must give their consent to non-face-to-face identification, and this consent must also be stored. The obliged entity must carefully consider precisely what identity verification documents and information are acceptable in non-face-to-face identification and ensure that the documents are undamaged and unaltered. Based on a risk assessment, it may be justified in non-face-to-face identification to request from certain customers additional clarifications and more detailed information.

Outsourcing non-face-to-face identification

Non-face-to-face identification is often purchased as a subcontract from an external service provider. Outsourcing non-face-to-face identification always requires the obliged entity to assess and carefully plan the risks associated with non-face-to-face identification. Procedures as well as the tasks and responsibilities of both parties must be specified in agreements. In addition, the obliged entity must require that customer relationship documentation be submitted to the obliged entity or that it be available to the obliged entity without delay throughout the customer relationship and the retention period provided for in the Money Laundering Act.

The obliged entity must ensure that it has sufficient technical competence, management understanding and continuity management in the outsourcing of non-face-to-face identification. The obliged entity accordingly must have the technical skills and competence to oversee and monitor the outsourced function. The obliged entity must also have a sufficient understanding of the outsourced function so that, if necessary, it can take over the handling of outsourced non-face-to-face identification itself or

[6] *Initial identification* refers to the verification of the identity of an applicant for a means of identification in connection with the issuing of the means. See the Act on Strong Electronic Identification and Electronic Trust Services (7.8.2009/617)

transfer it to a new service provider. The obliged entity is responsible for monitoring the quality of the service it has outsourced.

Responsibility for customer due diligence as well as compliance with ongoing monitoring and the obligation to obtain information and report remains with the obliged entity in all situations.

This document was drafted on 29.6.2021 by the AML/CFT Coordination Group's sub-group of supervisors established by the National Coordination Group on Combating Money Laundering and Terrorist Financing. For more information on the contents of the document, please contact the Financial Supervisory Authority. If you have any other queries, please consult your own supervisor under the Anti-Money Laundering Act.