HELLENIC REPUBLIC
CAPITAL MARKET COMMISSION

DECISION
4/894/23.10.2020
of the Board of Directors

Subject: Remote electronic identification of natural persons by the regulated entities by the Hellenic Capital Market Commission when entering into business relationships or carrying out occasional transactions

THE BOARD OF DIRECTORS
OF THE HELLENIC CAPITAL MARKET COMMISSION

Having considered:

1. Article 13 of Greek law 4557/2018 "Prevention and suppression of money laundering and terrorist financing (transposition of Directive 2015/849/EU) and other provisions" (Government Gazette A/139/30.7.2018),
2. Article 39 of the Legislative Act of 13 April 2020 "Measures to address the ongoing consequences of the COVID-19 pandemic, and other emergency provisions ((Government Gazette A/84/13.4.2020), as ratified by article 1 of Greek law (Government Gazette A/104/30.5.2020),
3. FATF guidance on digital identity (March 2020),
4. The Opinion of 23 January 2018 of the Joint Committee of the European Supervisory Authorities on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC/2017/81),
5. The Draft Guidelines of the European Supervisory Authorities under articles 17 and 18 (4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (“The Risk Factors Guidelines”), amending Guidelines JC/2017/37, of 4 January 2018,
6. FATF Guidance for a risk-based supervision to virtual assets and virtual asset service providers (June 2019),
7. Article 90 of Presidential Decree 63/2005 "Codification of the Legislation on Government and Governmental Bodies"(Government Gazette A/98/2005),
8. The fact that the provisions hereof do not cause for any expenses in the State Budget.

UNANIMOUSLY DECIDES

Article 1
Scope - subject matter

1. This decision shall apply:

a) to financial institutions of point (b) paragraph 1 of article 5 of Greek law 4557/2018,
b) to providers of exchange services between virtual currencies and fiat currencies of article 5 (1) (l) of Greek law 4557/2018, and
c) to the custodian wallet providers in operation, of article 5 (1) (m) of Greek law 4557/2018,

which are supervised by the Hellenic Capital Market Commission in accordance with article 6 (1) (b) of Greek law 4557/2018 (hereinafter the "Companies").

2. This decision lays down the terms and the conditions for the remote electronic identification of natural persons in the initiation of a business relationship with the Companies or carrying out occasional transactions These terms and conditions concern the reliable verification of identification data:

a) Full name and father's name
b) Identity card or passport number and issuing authority, and
c) Date and place of birth

according to identification documents set out in Annex I of the decision 1/506/8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission.

3. The provisions of this Decision shall also apply to the remote electronic identification of the beneficial owners of legal persons, as defined in Article 3(17) of Greek law 4557/2018, or the legal representatives of a legal person or other natural persons whose identity must be verified due to their relation with the legal person under the Annex I of the decision 1/506/8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission.

4. The terms and conditions laid down in this decision aim at mitigating the risk from entering into business relationships or carrying out occasional transactions without the physical presence of the customer. The validation of the customer's identity by the Police, Citizen Service Center, Consulate or other public authority, is equivalent to the validation made by the Companies where customers are physically present.

Article 2
Assessment and management of the risks of remote electronic identification

1. The Companies must ensure that the remote electronic identification process and the technological solution adopted are adequate and appropriate for the validation and verification of the identity of the natural persons on the basis of documents, data or information obtained from a reliable and independent source, as provided for by points (a) and (b) of paragraph 1 of article 13 of Greek law 4557/2018.

2. Where entering into business relationships or carrying out occasional transactions without physical presence the Companies must thoroughly assess the risks arising from the

remote electronic identification of natural persons in respect of the natural persons themselves, the reliability and independence of the sources for identity verification, the products or services to be provided to customers, as well as geographical and other factors. The Companies must adopt, on the basis of the above risk assessment, the appropriate remote electronic identification process and technological solution in line with the provisions of this decision and must ensure its effective implementation. When assessing the risks and establishing the applicable remote electronic identification process of natural persons, the Companies must have regard to the Opinion of 23 January 2018 of the Joint Committee of the European Supervisory Authorities on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC/2017/81).

Companies shall also take into account the relevant FATF guidance for Digital Identity. It is pointed out that in accordance with these guidelines, the entering into business relationships or carrying out occasional transactions, without the physical presence of the customer, through the use of a reliable digital identification system, does not automatically result in the business relationship or occasional transaction being classified as high risk, as it may be a normal and/or lower ML/TF risk relationship. The application of alternative methods of validating the identity of the customer must be taken to account by the Companies in the Risk Assessment Report they carry out in accordance with paragraphs 1 and 2 of article 35 of the Greek law 4557/2018, the point (d) of paragraph 2 of article 8 of decision 1/506/8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission and paragraph 10 of the European Supervisory Authorities Common Guidelines on Risk Factors (JC/2017/37).

3. The Companies must examine carefully the validity and authenticity of the data, documentation and information obtained in respect of natural persons as part of the remote electronic identification process, using an adequate range of data from different, reliable and independent sources, and bearing in mind that the data obtained electronically from the identity document of a natural person not physically present are not enough to verify his/her identity unless accompanied by the necessary control measures and mechanisms provided for in this decision.

4. Before adopting a remote electronic identification process and the relevant technological solution, the companies must conduct an informed assessment of:

a) the possibility of fully integrating the adopted technological solution into their existing systems, and the relevant technical and operational risks, and in particular the risk that the technological solution may be not reliable or could be tampered with or suffered irreparable failure,
b) qualitative risks, in particular the risk that the sources of information used for identity verification purposes are not sufficiently independent and reliable, as well as the risk that the extent of identity verification provided by the technological solution is not commensurate with the level of ML/TF risk associated with the natural person.
c) misuse of identity, i.e. the risk that the natural person is not who he/she claims to be or is not a real person, and
d) the risk that the technological solution does not comply with the applicable data protection legislation.

5. With respect to technical and operational risks, Companies must have sufficient in-house expertise, in addition to any external expert advice, to guarantee the proper implementation and use of the technological solution as well as to ensure the continuation of services should the technological solution suffer irreparable system failure or in case of termination of the business relationship between the Company and an external provider of the solution (where it is not developed in-house). To this end, the Companies must put in place proper contingency plans to ensure continuity of services.

6. The Companies must conduct appropriate tests in order to establish whether or not the remote electronic identification process and the technological solution are adequate and reliable and allow the application of the provided for in this decision customer due diligence measures in line with the Companies' AML/CFT policies and processes and the applicable AML/CFT legislation. To this end, the AML/CFT Officer referred to in article 38 of Greek law 4557/2018 must have a deep understanding of the workings of the technological solution and participate actively in its evaluation.

7. The above risk assessment and the remote electronic identification process must be approved by the Board of Directors of the Company, or by its senior management, as defined on a detailed recommendation from the relevant key function holders and the AML/CFT Officer referred to in article 38 of Greek law 4557/2018. Even if the process has been approved by the Board of Directors, senior management must have a deep understanding of these risks, the remote electronic identification process and the function of the technological solution.

8. The approved remote electronic identification process must include at least:

a) detailed description of the remote electronic identification process by method applied under article 3 and the organizational, technical and procedural safeguards that ensure the reliable identification and validation of the identity of natural persons and the management of the above relevant risks, as well as compliance with the provisions of this decision,
b) a procedure whereby additional measures and safeguards are triggered in the case of an insufficient degree of certainty as to the validity of an identity document or the identity of the natural person
c) a procedure for recording and monitoring any deviations from the approved remote electronic identification process, and
d) identification of unacceptable risk criteria and a procedure to terminate remote electronic identification process where such criteria are not met.

9. Companies must, on an annual basis, review the remote electronic identification process and the technological solution applied, having regard to technological developments, emerging risks and any changes in the AML/CFT framework, so as to ensure informed decision-making regarding their suitability and the need to introduce additional control measures and mechanisms as appropriate.

10. Companies must without undue delay remedy any errors or weaknesses in the remote electronic identification process and the technological solution, as may be identified at any time or during a regular review, also taking the following additional actions:

a) a review of all affected business relationships, to assess whether sufficient customer due diligence (CDD) has been applied to such relationships, in line with the Company's policies and processes,

b) an assessment, after the weaknesses have been corrected and adequate CDD has been applied, of whether any affected business relationships can be maintained or should be terminated, and/or the execution of transactions related to such business relationships should be stopped, and

c) an assessment of whether or not, further to the above actions, a report should be submitted to the AML/CFT Authority referred to in article 4 of Greek law 4557/2018.

Where the Companies have identified serious weaknesses in the technological solution or systematic errors related to its use, they must comprehensively examine the level of reliability of the technological solution against the ML/TF risks involved, the scope for improvements to the solution and the continuation or discontinuation of its use, on the basis of their business continuity plans.

11. The companies must ensure that their internal audit functions conduct specific audits to verify the suitability, adequacy and reliability of the remote electronic identification process and the technological solution used. The outcome of such audits must be notified to the AML/CFT Officer referred to in article 38 of Greek law 4557/2018, in the context of the monitoring and assessment of the implementation of AML/CFT policies and processes, and must be included in the latter's annual report. The suitability, adequacy and reliability of the remote electronic identification process and the technological solution must also be audited by the external auditors and the outcome of such audits must be included in their report, prepared in accordance with the provisions of article 9 of the decision 1/506/8.4.2009 of Board of Directors of the Hellenic Capital Market Commission.

12. The companies must be in a position to prove to the Hellenic Capital Market Commission the suitability, adequacy and reliability of the remote electronic identification process and the technological solution adopted for this purpose, whether or not they have outsourced it, wholly or partly.

Article 3
Permitted methods of remote electronic identification

1. The following remote electronic identification methods shall be permitted to companies:

a) video conference with a trained employee, using software applications, such as Microsoft Teams, Skype, WebEx, Zoom or other application, in order to verify the "physical existence" of the client with that shown in the documents received by e-mail during the video conference. This method consists in an interactive, real-time audiovisual communication between a natural person and a trained employee who are in different locations and supports the exchange of files and messages,

b) automatised identification via a dynamic selfie, without the physical presence of an employee, taken by the natural person in real time (as opposed to a static selfie), so as to ensure liveness detection.

2. For the purposes of remote electronic identification, original identity documents among those referred to in Annex I of the decision 1/506/8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission, shall be accepted, provided that they are included in the Public Register of Authentic travel and identity Documents Online (PRADO) of the European Council and the Council of the European Union, and bear:

a) photograph and signature of the holder, and
b) a machine-readable zone (MRZ), and
c) two additional advanced visual security features among those specified in PRADO.

3. By exception to preceding paragraph 2, companies may, after assessing the risk involved, accept as identity document of Greek citizens an ID card issued by the Hellenic Police with the full name written also in Latin characters, provided that the following conditions are met:

a) exclusively as part of the video conference method with a trained employee, and
b) subject to ID card authenticity check through the Central Portal of Public Administration, in accordance with article 39 of the Legislative Act of 13 April 2020 "Measures to address the ongoing consequences of the COVID-19 pandemic, and other emergency provisions (Government Gazette A/84/13.4.2020), as ratified by article 1 of Greek law (Government Gazette A/104/30.5.2020),

In addition, subject to the prior point (a), the Companies may accept as identity documents of Greek citizens a passport in force and a military ID card if these documents are included in the Central Portal of Public Administration.

4. Where companies apply the remote electronic identification process, without the physical presence of an employee, supported by dynamic selfie identification using specialized software application, they must also take one of the following additional risk mitigation measures:

a) They must ensure that the first credit wire transfer to the natural person's account is made from an account kept in his/her name with a credit or financial institution situated in an EU Member State or a FATF member country. Companies may, alternatively, confirm the existence of the above account by obtaining information from the account-holding credit or financial institution itself, as well as from any other reliable and independent source.
b) They impose a limit of fifteen thousand euros (€15,000) on the total credits (deposits of funds and/or financial instruments) to be carried out per year on behalf of the natural person.

Article 4
Control measures and mechanisms in connection with remote electronic identification

1. Companies must have in place control measures and mechanisms to ensure the reliability of the remote electronic identification process of natural persons, regardless of the method applied, as follows::

a) Companies must adopt advanced technical specifications for the verification of the authenticity, validity and integrity of identity documents, making sure that they have not been altered or falsified in any manner whatsoever (e.g. by changing data of a genuine document, reproducing a genuine document, creating a fraudulent identity document

using materials from legitimate documents). To this end, companies must check the submitted identity documents against the specifications of each document included in Public Register of Authentic travel and identity Documents Online (PRADO) of the European Council and the Council of the European Union, in particular the security features, type, size of characters and structure of the document. Moreover, companies must verify the authenticity of the identity document on the one hand by reading and decrypting the information included in the MRZ and, on the other hand, by checking another two visual security features of those referred to in paragraph 2 of article 3 of this decision.

b) They must ensure the reliability of the remote electronic identification process by relying, to the extent possible, on multiple alternative information sources. The reliability of the remote electronic identification process is enhanced when companies draw data from the Central Portal of Public Administration or other reliable and independent sources and databases in order to verify information or data obtained during the remote electronic identification process.

c) They must perform consistency checks against the natural person's profile, identity document and any other information about the natural person, using an adequate range of data from reliable and independent sources.

d) They must dynamically develop the remote electronic identification process by designing a sufficient number of alternative standard identification scenarios and choosing randomly one of them.

2. Companied must adopt technical measures and safeguards in the remote electronic identification process of natural persons, regardless of the method applied, as follows:

a) They must implement techniques of secure communication between the Company and the natural person, ensuring the integrity and confidentiality of the information exchanged.

b) They must ensure that the remote electronic identification process occurs in real time and without interruptions and that no files created by the natural person in any manner before the initiation of the process are accepted.

c) They must ensure that any photographs and videos taken during the remote electronic identification process are of such quality that both the natural person and the data on his/her identity document are fully and unambiguously recognisable. Moreover, they must ensure that during the remote electronic identification process there are proper lighting conditions, the natural person has the proper distance from the camera, without anything covering his/her face, and his/her required features are captured with absolute clarity.

d) They must ensure that all the data received, as well as the results of the controls conducted in the various stages of the remote electronic identification process, are kept on a digital record, properly protected from any attempt at tampering. These data must include any photograph or video taken during the remote electronic identification process.

e) They must ensure that a single device is used throughout the remote electronic identification process.

3. As part of the remote electronic identification process and regardless of the method applied, Companies must apply specific measures and controls, supported by dedicated media:

a) They must take photographs/snapshots, in proper lighting conditions, showing clearly:
aa) the face of the natural person under different angles, e.g. in profile, face on, using in parallel techniques to ensure liveness detection (such as eyes opened, eyes shut),
ab) the pages/sides of the identity document that bear the photograph, signature and identity data of the natural person, so as they can be checked against the specifications and security features of the document.
b) They must use biometric algorithms to compare the natural person with the photograph on the identity document.
c) They must require the natural person to enter a unique number sent by email or SMS.
d) They must collect additional data, such as geolocation, IP address of the customer's computer and/or verifiable telephone numbers, in order to verify the data provided by the customer.

4. In the context of the video conference with a trained employee method of remote electronic identification of a natural person, Companies must, in addition to the above:
a) ask the natural person to place a finger over the security zone of the document or move his/her hand in front of his/her face,
b) in the case of ID cards issued by the Hellenic Police, also check whether the card lamination has been damaged or tampered with, or there are indications of attempted falsification of the document, or whether the photograph was inserted into the document after its issuance, and
c) conduct investigation in order to identify any suspicious behavior of the natural person that may indicate that he/she is under the influence of substances or is under duress or is mentally deranged.

Article 5
Termination of the remote electronic identification process

1. Companies must ensure that the remote electronic identification process is terminated without being completed in any of the following cases:
a) the visual validation of the natural person and/or the official identity document is not possible, as defined above, or there is any inconsistency or uncertainty, or
b) there is any discrepancy between the data and information submitted during the remote electronic identification process and the data obtained from a reliable and independent source, or
c) the unacceptable ML/TF risk criteria laid down by the Company are met, in accordance with point (d) of paragraph 8 of article 2 of this decision.

2. The reason of termination of the remote electronic identification process must be recorded and kept in an adequately protected record for a period of at least five years, in accordance with Article 30 of Greek law 4557/2018 and of article 8 of this decision.

Article 6
Organisational arrangements and staff training

1. Companies must ensure that the remote electronic identification process is conducted by qualified and trained staff, to whom they shall make available the necessary resources and special technical media for the smooth and secure implementation of the process. Training

must include the practical application of the technological solution and its functionalities, the security features of acceptable identity documents, common counterfeiting and falsification methods, the requirements of this decision, identification of unusual or suspicious transactions and reporting in line with the Company's internal procedures. Training shall take place before the staff assumes relevant duties, shall be repeated regularly and shall be provided in addition to the general AML/CFT training under the applicable institutional framework.

2. Companies shall ensure through appropriate procedures that the staff engaged in the identification and validation of customers through the technological solution do not collaborate with persons involved in illegal activities. These procedures shall include pre-hire and regular on-the-job fit for duty assessment; random assignment of natural persons' applications for remote electronic identification to the staff, so as to minimise manipulation risk; and sample checks of the staff's communications with natural persons during or after the remote electronic identification process.

3. Where Companies apply the video conference method for remote electronic identification, they shall ensure that the staff engaged are located in a specially designed area with restricted access.

Article 7
Outsourcing of the remote electronic identification process to an external service provider

1. If Companies decide to outsource, wholly or partly, the remote electronic identification process, they shall ensure, through appropriate assessment and control procedures, that the external service provider has adopted appropriate technical specifications and safeguards ensuring reliable identification and validation of the identity of natural persons, in line with the Company's remote electronic identification process. In any case, the ultimate responsibility for complying with the provisions of this decision and the requirements of the AML/CFT framework shall rest with the Company. Such responsibility shall include the ongoing monitoring of the efficiency and reliability of the remote electronic identification process, and granting explicit prior approval of any modification of the process by the external service provider.

2. Companies must ensure that the external service provider is contractually bound to perform its duties under the cooperation contract in compliance with the provisions of this decision and the institutional framework applicable from time to time. The outsourcing agreement shall set out clearly and in detail the roles, responsibilities, rights and obligations of each party, including those arising from expiry of the agreement or earlier termination thereof, in which case an exit plan shall be activated including the transfer of any information and data obtained by the external service provider in the performance of the agreement. The outsourcing agreement shall explicitly provide that no change to the remote electronic identification process is possible without the prior approval of the Company.

3. Companies shall ensure that the external service provider:

a) provides adequate and accurate information on the information sources used, the controls conducted and the outcomes of the remote electronic identification process for every natural person, enabling the Company to assess the quality of the process and establish the reliability of identification and verification,

b) complies with the personal data protection legislation and adopts adequate information security standards, and
c) uses qualified and trained staff in the remote electronic identification process. Training shall include the implementation of the technological solution and its operating potential; the security features of acceptable identity documents; common counterfeiting and falsification methods; the requirements of this decision; and identification of unusual or suspicious transactions.

4. Where the external service provider is situated in a third country, Companies must have a good understanding of and address effectively the associated legal and operational risks and data protection requirements. Companies are not allowed not hire external service providers situated in a third country, which has been identified by the European Commission as a high-risk country for ML/TF as well as in a third country that has in place legal restrictions that do not allow the free exchange of information between the external service provider and the Company or the Hellenic Capital Market Commission, or the external service provider's compliance with the AML/CFT framework.

5. The execution, in whole or in part, of the remote electronic identification process by an external service provider and the latter's relation with the Company may under no circumstances jeopardise the operation and quality of the Company's internal control system and the ability of the Hellenic Capital Market Commission to check, at such time and in such manner as it may deem expedient and appropriate, the Company's compliance with the obligations arising from the provisions of this decision.

Article 8
Record keeping and personal data protection

1. Companies must comply with the record keeping requirements of articles 30 and 31 of Greek law 4557/2018 and this decision, as well as the personal data protection legislation, regardless of the type or external provider of the technological solution they use in the remote electronic identification process.

2. Companies must keep intact all the necessary records/data allowing them to determine the exact date when documents are submitted and information and data are received during the remote electronic identification process.

3. Companies must ensure that natural persons are informed about the processing of their personal data. With regard to biometric and remote electronic identification, the explicit and specific consent of natural persons must be required.

Article 9
Transitional provisions

1. For as long as Companies are not connected with the Central Portal of Public Administration, the provisions of point (b) of article 3(3) shall not apply in respect of verification of the authenticity of a natural person's ID card issued by the Hellenic Police through this interface.

2. The Special Unit for the Prevention of Money Laundering of the Hellenic Capital Market Commission is authorised to provide clarifications and instructions regarding the implementation of this decision.

Article 10
Entry into force

This decision shall enter into force as from its publication in the Government Gazette.

This decision shall be published in the Government Gazette.

The Secretary

Alexandra Ninasiou

President	The 1st Vice-Chair	The 2nd Vice-Chair
Vassiliki Lazarakou	Nikolaos Kontaroudis	Anastasia Stamou

The members

Anastasios Virvilios	Panagiotis Giannopoulos
Christina Papakonstantinou	Spyridon Spyrou