(**AUTOMATIC TRANSLATION**)
DECISION
4/894 / 23.10.2020
of the Board of Directors

Subject: Remote electronic identification of individuals by supervised by the Hellenic Capital Market Commission persons when concluding business relationships or occasional transactions

THE BOARD OF DIRECTORS
OF THE CAPITAL MARKET COMMISSION

Taking into consideration:

1.
Article 13 of Law 4557/2018 "Prevention and suppression of money laundering from criminal activities and terrorist financing (integration of Directive 2015/849 / EU) and other provisions "(Government Gazette A / 139 / 30.7.2018),

2.
Article 39 of the Legislative Content Act of 13.4.2020 "Measures for addressing the ongoing consequences of the COVID-19 coronavirus pandemic and other urgent provisions "(Government Gazette A / 84 / 13.4.2020), as ratified by article 1 of law. 4690/2020 (Government Gazette A / 104 / 30.5.2020),

3.
Articles 24-30 of the Legislative Content Act of 20.3.2020 "Urgent measures to address the consequences of the risk of spreading COVID coronavirus; 19, supporting society and entrepreneurship and ensuring smooth running market operation and public administration "(Government Gazette A / 68 / 20.3.2020), as ratified with article 1 of law 4683/2020 (Government Gazette A / 83 / 10.4.2020),

4.
The FATF Digital Identity Guidelines (March 2020),

5.
The Opinion of the Joint Committee of the European Supervisory Authorities dated 23.1.2018 on the use of innovative solutions by credit and financial institutions organizations in the due diligence process (JC / 2017/81),

6.
The Draft Joint Guidelines of the European Supervisory Authorities in accordance with Articles 17 and 18 (4) of Directive (EU) 2015/849 due diligence measures and the factors to be considered credit institutions and financial institutions at its discretion risk of money laundering and financing terrorism linked to individual business relationships and occasional transactions (Risk Factors Guidelines), which amend the 4.1.2018 Guidelines JC / 2017/37,

7.
The FATF Guidelines for risk-based supervision virtual assets and virtual service providers assets (virtual asset service providers) (June 2019),

8.
Article 90 of p.d. 63/2005 "Codification of the legislation for the Government and the governmental bodies "(Government Gazette A / 98/2005),

9.
The fact that the provisions of this do not cause any expense to him State Budget,

DECIDES UNANIMOUSLY

Article 1
Scope - object

1.

This Decision shall apply:
a)
to the financial institutions of case b of par. 1 of article 5 of n. 4557/2018,
b)
to virtual currency exchange service providers and of documentary coins of circumstance l of par. 1 of article 5 of law 4557/2018 and
c)
to the providers of digital wallet custody services in its area par. 1 of article 5 of law 4557/2018, which are supervised by the Hellenic Capital Market Commission in accordance with circumstance par. 1 of article 6 of law 4557/2018 (hereinafter, cumulatively, the "Companies").
2.
This decision determines the terms and conditions for the remote electronic identification of individuals when entering into a business relationship with the Companies or conducting an occasional transaction. These terms and conditions relate to the reliable verification of the following certification data of identity:
a)
Name and patronymic,
b)
Identity card or passport number and issuing authority and
c)
Date and place of birth on the basis of the identification documents set out in Annex I to 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 in the case of ex distance of electronic identification of the real beneficiary of a legal entity, against the meaning of par. 17 of article 3 of law 4557/2018, or legal representative of a legal person or other natural person whose verification and verification is required of his identity due to his relationship with a legal entity under Annex I thereof Decision 1/506 / 8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission.
4.
The terms and conditions provided for in this Decision are intended to mitigation of the risk arising from the conclusion of a business relationship or conduct occasional transaction without the physical presence of the customer. Its certification of the customer by the Police, Citizens' Service Center, Consulate or another public Authority, is equivalent to the certification made by the Companies to customers with physical presence.

Article 2
Risk assessment and management
of remote electronic identification

1.
Companies ensure that the process of remote electronics identification of individuals and the technological solution they adopt are sufficient and suitable for verifying and verifying the identity of natural persons on the basis of documents, data or information from a reliable and independent source, such as provide for circumstance α΄ and β΄ of par. 1 of article 13 of law 4557/2018.
2.
In the case of entering into a business relationship or conducting an occasional without physical presence the Companies carry out a thorough evaluation of risks arising from the remote identification of natural persons and related to individuals themselves, the reliability and independence of sources

verifying their identity, the products or services they will receive, and with geographical and other factors. The Companies adopt, based on the above risk assessment, the appropriate procedure and technological solution for the remote electronic identification of natural persons, according to forecasts of this Decision, and ensure its effective implementation. During the risk assessment and

determination of the applicable procedure of ex distance electronic identification of individuals, the Companies take into account on 23.01.2018 Opinion of the Joint Committee of the European Supervisory Authorities on by using innovative solutions in the due diligence process from credit institutions and financial institutions (JC / 2017/81).
The Companies also take into account the relevant FATF Guidelines for Digital Identity. It is noted that according to these Guidelines, the starting a business relationship or conducting an occasional transaction without the physical in the presence of the customer, through the use of a reliable digital identification system, no automatically characterizes the business relationship or casual transaction as high risk as it may be a normal and / or relationship lower risk ML/TF. The application of alternative methods of its verification customer identity is taken into account by the Companies in the Valuation Report Risks carried out in accordance with par. 1 and 2 of article 35 of law 4557/2018, the par. d of par. 2 of article 8 of decision 1/506 / 8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission and par. 10 of their Common Guidelines European Supervisors for Risk Factors (JC / 2017/37).
3.
The Companies carefully examine their validity and authenticity documents, data and information obtained during the process of ex distance electronic identification of natural persons and use adequate data from different, reliable and independent sources, taking into account that data collected electronically through its identity documents natural person, without its physical presence, is not sufficient to verify it if they are not accompanied by the necessary measures and control mechanisms provided for in this Decision.
4.
The Companies, before the adoption of the distance electronics process identification of the natural persons and the technological solution, evaluate documented:
a)
the possibility of full integration of the adopted technological solution in existing systems and processes and related technological and operational risks, and in particular the risk that the technological solution may not be reliable or may be breached or irreparably damaged,
b)
the quality risks, especially the risk the sources of information that used for authentication purposes may not be sufficient independent and reliable, as well as the risk the degree of its reliability process of remote electronic identification through technological not be proportionate to the level of ML/TF risk associated with the natural person,
c)
the risk of fraud due to impersonation, ie the risk to the natural person not to be what it claims to be or not to exist and
d)
the risk that the adopted technological solution will not meet its forecasts legal framework for the protection of personal data.
5.
In terms of technical and operational risks, the Companies, regardless of the external consulting services they may receive, they have themselves internally sufficient know-how to be able to ensure proper implementation and use of the technological solution, as well as the continuation of the services provided in in case the technological solution suffers irreparable system damage or in case

that for any reason the relationship between the Company and its external provider technological solution is interrupted. For this purpose, the Companies develop appropriately work continuation plans.
6.
Companies conduct appropriate tests to determine the process of remote electronic identification and the technological solution they will adopt are adequate and reliable and allow the application of the provisions of this Decision on due diligence in accordance with policy and procedures of the Company and the institutional framework for the prevention of ML/TF. For this purpose, the Competent Manager of article 38 of law 4557/2018 fully understands the mode of operation

of the technological solution and actively participates in its evaluation.
7.
The above risk assessment and the process of remote electronics identification of natural persons are approved by the Board of Directors of the Company, on the basis of a detailed recommendation of the Competent Executive Officer of Article 38 of the Law 4557/2018. In addition to the approval by the Board of Directors, the management of the Company fully understands these risks, the process of remote electronic identification of individuals and how the technological solution works.
8.
The above approved procedure of remote electronic identification natural persons shall include at least the following:
a)
detailed recording of the various stages of the remote process electronic identification by method used in Article 3 and organizational, technical and procedural measures to ensure credibility identification and verification of natural persons and treatment of the above related risks, as well as compliance with its provisions of this Act,
b)
process for activating additional security measures and valves in cases of unsatisfactory degree of certainty as to its validity identification document or the identity of the natural person,
c)
process of recording and monitoring the discrepancies carried out in in relation to the approved remote electronic identification procedure and
d)
identification of unacceptable risk criteria and its termination process procedure for remote electronic identification in the event that these criteria are met.
9.
The Companies re-evaluate the process of distance on an annual basis electronic identification of individuals and the technological solution they apply, taking into account technological developments, emerging risks and any changes to the institutional framework ML/TF prevention to ensure reception informed decisions as to their appropriateness and the need for implementation additional control measures and mechanisms, as appropriate.
10.
The Companies immediately correct the errors and weaknesses of its process remote electronic identification of individuals and the technological solution which they locate, at any time or during the regular annual minimum re-evaluation, in addition to the following sub-actions:
a)
overview of affected business relationships in order to assess whether due diligence measures have been adequately implemented in accordance with them with the policies and procedures of the Company,
b)
evaluation, after checking the adequate implementation of the due diligence measures and addressing relevant shortcomings, if the affected business relationships can be maintained or must be terminated and / or if the performance related transactions must be stopped and

c)
assessment whether, following the above steps, reference should be made to Principle of article 47 of law 4557/2018.
In case the weaknesses of the technological solution are serious or the errors from its use is systematic, the Companies review the overall level of reliability in relation to the risks involved ML/TF, the possibility of improvements and the continue or not to use it, based on their work plan.
11.
The Companies ensure that their Internal Auditor proceeds to specialized checks to determine suitability, adequacy and reliability the applicable remote electronic identification procedure and technological solution. The results of the audits are brought to the attention of the Competent

Executive of article 38 of law 4557/2018, in the context of monitoring and evaluating the effective implementation of policies and procedures ML/TF prevention and are included in its Annual Report to the Administration Council. The evaluation of its suitability, adequacy and reliability the process of remote electronic identification and technological solution is subject to control by both external auditors and included in their report, drawn up in accordance with the provisions of Article 9 of the decision 1/506 / 8.4.2009 of the Board of Directors of the Hellenic Capital Market Commission.

12.

The Companies are in any case able to document to the Commission Capital market the adequacy, suitability and reliability of the applied remote electronic identification process and the technological solution that have adopted for this purpose, irrespective of the assignment of part or all of it to an external service provider.

Article 3
Permitted methods of remote electronic identification

1.

The permitted methods of remote electronic identification, which may be applied separately by the Companies, are the following:

a)

teleconferencing with a trained employee, using software applications, such as Microsoft Teams, Skype, WebEx, Zoom or another application, in order to verify the "physical condition" of the customer with that which appears in documents received by email during of video conferencing. This method is two-way visual and audio Real-time communication between the natural person and trained staff located in different locations and which also supports the exchange of files and messages,

b)

automated process without the presence of an employee, through dynamic self-portrait (dynamic-selfie) in real time with the use of specialized software application, which is based on dynamic rather than static photos taken of the natural person to ensure a live participation in the process (liveness).

2.

Prototypes are accepted for remote electronic identification documents listed in Annex I to Decision 1/506 / 8.4.2009 Board of Directors of the Hellenic Capital Market Commission, provided that they are included in Online Public Register of Genuine Identity and Travel Documents (PRADO) of European Council and the Council of the European Union and bear:

a)

photo and signature of their holder and

b)

machine readable zone (Machine Readable Zone-MRZ), as well as

c)

two more advanced optical security features than those
are described in detail in the above register.

3.

Except as provided in paragraph 2, the Companies may, accordingly risk assessment to be accepted as a document identification of Greek citizens the Police Identity Card, in which the name is also written in Latin characters, under the following conditions:

a)

application exclusively of the teleconferencing method with a trained employee and

b)

confirmation of the authenticity of the police ID card of the natural through an interface with the Single Digital Portal of Public Administration, in accordance with the provisions of article 39 of the Legislative Act of 13.4.2020 Content "Measures to address its ongoing consequences of the COVID-19 coronavirus pandemic and other emergency provisions "(Government Gazette

A / 84 / 13.4.2020), as ratified by article 1 of law 4690/2020 (Government Gazette A / 104 / 30.5.2020).
Also, subject to the above circumstance, the Companies may accept as identification documents of Greek Citizens Passport in force and Identity of employees to the Security Forces and the Armed Forces if these documents are included in the Single Digital Portal of Public Administration.
4.
In the event that the Companies apply the method of automated electronic identification distance without the presence of an employee, by receiving potential dynamic selfie using specialized application software, take an additional one of the following ML/TF risk mitigation measures:
a)
Ensure that the first credit in the account of the natural person is made from an account held in his name by a credit institution or a financial institution established in a European Member State Union or in a third FATF member country. Companies may, alternatively, confirm the existence of the above account through information that is verified by the credit institution or financial institution in which it is observed, as well as in another credible and independent manner.
b)
They impose a limit of fifteen thousand euros (€ 15,000) on all credits (deposits of funds and / or financial instruments) carried out per year on behalf of the natural person.

Article 4
Control measures and mechanisms
of the remote electronic identification process

1.
The Companies adopt the following measures and control mechanisms to ensure the reliability of the remote electronic identification process used natural persons, regardless of the method used:
a)
Adopt advanced technical specifications for authentication, the validity and integrity of the identification documents, checking that they do not bear any indication of falsification or falsification of any kind (such as by changing authentic document elements, by replicating the original document or by creating a fraudulent document using legal elements / materials document). For this purpose, the Companies compare the submitted documents identification with the specifications of each document contained in Online Public Register of Genuine Identity and Travel Documents (PRADO) of the European Council and of the Council of the European Union and in particular in terms of security features, type, size characters and the structure of the document. In addition, the Companies confirm the authenticity of document identification, on the one hand, reading and decrypting the information contained in the machine readable zone (MRZ) and on the other hand, controlling at least two more visually characteristics in accordance with paragraph 2 of Article 3 hereof.

b)
They ensure the reliability of the remote electronics process identification, based as far as possible on multiple and alternative sources information. The reliability of the electronic identification process is enhanced when the Company obtains data through the Unified Public Digital Portal Administration or from other reliable and independent sources and databases for verification of information or data obtained in the course of the proceedings electronic identification.
c)
They carry out tests of logical consistency in relation to the characteristics of the physical identification document and any other physical information person, using a sufficient range of data from reliable and independent sources.
d)
They dynamically shape the structure of the remote electronics process identification, developing a sufficient number of different standardized scenarios identification, by randomly selecting one of them.
2.
The Companies adopt the following measures of a technical nature and safety valves against

the process of remote electronic identification of natural persons, regardless of the method used:
a)
They apply secure communication techniques between the Company and the individual ensuring the integrity and confidentiality of the migrant information.
b)
Ensure that the process of remote electronic identification takes place in real time and without interruption and that they are not accepted files that have been created by the natural person in any way before the start of the procedure.
c)
Ensure that photos and videos are taken during the remote electronic identification process is of such quality so that both the natural person and the information contained in the document be fully identifiable and indisputable. In addition, ensure that during the electronic identification process there are suitable lighting conditions, the natural person maintains suitable distance from the camera, does not cover his face and that is achieved in the unmistakable imprint of its required characteristics is born.
d)
Ensure that all data recorded is digitally recorded as well as the results of the checks carried out at individual stages of the remote electronic identification process, which is adequately protected from any attempt to alter its content. This data includes any photo or video is taken during the remote electronics process identification.
e)
Ensure that the process of remote electronic identification carried out using a single device throughout its duration.
3.
The Companies during the process of remote electronic identification natural persons and regardless of the method used, apply the following specifically measures and controls, with the support of specialized technological instruments:
a)
They take under appropriate lighting conditions photos / snapshots that illustrate clearly:
aa)
the face of the natural person from different angles, such as for example from the side (profile) and from the front (en face), using parallel techniques that suggest that the subject participates live in procedure (liveness, such as eyes open / eyes closed),
ab)
the faces of the identification document containing the photograph, the signature and his identity in order to carry out the verification in relation to the specifications and security features of the document.

b)
Carry out checks on the biometric characteristics of the natural person, in relation to the photo of the identification document, using special software.
c)
They ask the natural person to enter a unique number, which he receives with e-mail and / or text message (SMS) on his mobile phone.
d)
They receive additional information, such as geolocation, IP address the client's computer and / or verifiable telephone numbers, in order to verify the information provided by the customer.
4.
If during the process of remote electronic identification of a physical apply the method of teleconferencing with a trained employee, the Companies, in addition to the above:
a)
ask the natural person to place his finger in front of them security features of the identification document or move the hand in front of his face,
b)

check, in addition, in the case of the Hellenic Police Bulletin Identity, whether the lamination used for its sealing document has been damaged or damaged or there is evidence of an attempt forgery of the document, as well as whether the photograph has incorporated in the document after its issue and

c)

carry out checks to detect any suspicious behavior of the natural of a person who may indicate that he is under the influence of substances or that he is under duress or possible mental or intellectual disorder.

Article 5

Termination of the remote electronic identification process

1.

Companies ensure that the process of remote electronics is terminated without being completed if at least one of the following circumstances:

a)

it is not possible to visually confirm the natural person or the official identification document or both, as defined above, or exists any disagreement or uncertainty between them or

b)

there is any discrepancy between the data, information and data which submitted during the remote electronics process identification with an independent and reliable source or

c)

the unacceptable risk criteria ML/TF identified by Company, according to the provisions of circumstance d of par. 8 of article 2 of the present.

2.

The reason for terminating the remote electronic identification process is recorded and kept in a sufficiently protected file for a period of time at least five (5) years, according to article 30 of law 4557/2018 and the provisions in Article 8 of this Decision.

Article 6

Organizational arrangements and staff training

1.

Companies ensure that the process of remote electronics identification is carried out by appropriate and specially trained personnel, in which have the necessary resources and specialized technical means for the seamless and secure implementation of the process. The training includes practical application of the technological solution and its functional capabilities, security features the identification documents accepted, as well as the usual methods falsification or falsification thereof, the requirements of this Decision, and the detection of unusual or suspicious transactions and the transmission of relevant reports,

in accordance with the internal procedures of the Company. The training takes place before the assumption of staff duties, is repeated at regular intervals and is provided in addition to general training to combat ML/TF according to the relevant institutional framework.

2.

The Companies ensure through appropriate procedures th at the staff that conducts the verification and verification of the identity of the customers through the technological does not cooperate with persons involved in illegal activities.

These procedures include checking the suitability of staff before recruitment and regular evaluation thereafter, random assignment to personnel of electronic identification requests of natural persons in order to the possibility of manipulation of the process is minimized, and the sampling control of staff communications with natural persons during its execution process of remote electronic identification or after its completion.

3.

If the Companies apply the method of remote electronics natural person identification by teleconferencing, ensure that staff who is to be installed in a specially designed limited space and controlled access.

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

1.
In case the Companies assign to an external service provider the performing part or all of the remote electronic identification process ensure, through appropriate evaluation and control procedures, that the external service provider has adopted appropriate technical specifications; and safety valves that ensure its reliable verification and verification identity of natural persons, in accordance with the procedure of remote electronics identification of natural persons of the Company. In any case, the ultimate responsibility for compliance with the provisions of this Act and the requirements of the institutional framework ML/TF prevention is the responsibility of the Company. This responsibility includes ongoing monitoring the effectiveness and reliability of its process remote electronic identification by the Company and its explicit approval Company before any modification of the one applied by the external provider procedure.
2.
The Companies ensure that the external service provider is contractually committed perform the required duties arising from the contract between them in accordance with the provisions of this Decision and of each case existing institutional framework. The cooperation agreement clearly describes and detail the roles, responsibilities, rights and obligations of each party, including those arising from the termination or termination of the contract, either due to the expiration of its validity period, or exceptionally at an earlier time, in which case the exit plan is activated, which includes the transfer of any data and data have been obtained from the external provider during its execution contract. The cooperation agreement explicitly states that there will be no change in process of remote electronic identification without prior approval the company's.
3.
The Companies also ensure that the external service provider:
a)
provides sufficient and accurate information on the sources of information that used, the tests performed and the results of ex distance electronic identification process for each individual, thus

so that the Company is able to evaluate the quality of the process and to the reliability of the verification and verification of his identity is documented natural person,
b)
complies with the legal framework for the protection of personal data and adopts adequate information security standards and
c)
uses appropriate and specially trained staff for the electronic identification distance. Training includes practice implementation of the technological solution and its operational capabilities, the security features of the identification documents accepted, as well as the usual methods of falsification or falsification thereof, requirements of this act and the detection of unusual or suspicious transactions.
4.
In case the external service provider is installed on a third party country, the Companies understand the legal and operational risks and requirements data protection associated with them and deal with them effectively.
Companies are prohibited from contracting with an external service provider established in a third country, which has been identified by the European Commission as a high risk country ML/TF as well as in a third country in which there are legal restrictions, which are not allow the smooth exchange of information between, on the one hand, the provider and on the other hand of the Company or the Hellenic Capital Market Commission, or the Company's compliance with the institutional framework of prevention ML/TF.
5.

Execution of part or all of the process remotely electronically identification by an external provider and its relationship with the Company is prohibited to endangers in any way the operation and quality of the mechanism internal control of the Company and the possibility of the Hellenic Capital Market Commission to check, at any time and in any way - which she deems appropriate and appropriate where applicable - the Company's compliance with the obligations arising from provisions of this Decision.

Article 8
Record Keeping and Personal Data Protection

1.
The Companies comply with the obligations of articles 30 and 31 of the law. 4557/2018 and this decision, as well as the legal framework for protection personal data, regardless of the type and provider of the technological solution used for remote electronic identification of individuals.
2.
The Companies keep all the necessary records that allow them to specify the exact date of submission of documents, information and data received in the process of remote electronics identification of natural persons.
3.
The Companies ensure that individuals are informed about processing of their personal data. Especially for the control of biometrics their characteristics and their remote electronic identification, of course persons provide explicit and specific consent.

Article 9
Transitional provisions

1.
During the period that has not been provided to Companies the possibility with the Single Digital Portal of Public Administration, the

provided in circumstance b) of par. 3 of article 3 regarding its confirmation authenticity of the Police Identity Card of the natural person through the en due to interconnection.
2.
The Special Service Unit for the Treatment of Money Laundering from Criminal Activities of the Hellenic Capital Market Commission is authorized to provide clarifications and instructions for the implementation of this Decision.

Article 10
Entry into force

This Decision shall enter into force upon its publication in the Government Gazette.
This Decision to be published in the Government Gazette.

The Secretary Alexandra Ninasiou

The President Vasiliki of Lazarakou

The First Vice President Nikolaos Kontaroudis

The Second Vice President Anastasia Stamou

The members
Anastasios Virvilios
Panagiotis Giannopoulos
Christina Papakonstantinou
Spyridon Spyrou