MAGNETIQ BANK

Magnetiq Bank General Terms of Remote Client Identification

Version 4

Riga, 25.09.2025

MAGNETIQ BANK

Terms and Definitions:

PEP Close Associate – an individual known to have a business or other close relationship to a PEP, a shareholder or participant in the same company as a PEP, or an individual being the sole owner of a legal entity known to have been established for the actual benefit of a PEP.

Banka – AS Magnetiq Bank, registered in the Republic of Latvia under uniform registration No. 50103189561, registered office: Brīvības iela 54, Rīga, LV-1011, E-mail address: info@magnetiqbank.com, website address: www.magnetiqbank.com, BIC/SWIFT: LAPBLV2X. The Bank has been issued a licence for conducting credit institution activities, and its operations are overseen by the Bank of Latvia. The address of the Bank of Latvia is K.Valdemāra iela 2a, Rīga, LV-1050.

Cenrādis – the service price list approved by the Bank, as valid on the date of executing a specific operation of the Bank and available at points of service and on the Bank's website: www.magnetiqbank.com.

Secure Electronic Signature – qualified electronic signature within the meaning of Article 3(12) of 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 (hereinafter referred to as 'Regulation (EU) No 910/2014.

Photo identification – the comparison of an image of an identity document with an electronic self-portrait (selfie) photograph, in accordance with the requirements of the Applicable Law.

Identifiable person – the Client, the Client's representative at the Bank, an Additional payment card user, an Internet Banking user, an E-commerce service client, or any other person subject to Remote Identification in accordance with the Rules.

ICT Service Provider No. 1 – SumSub Tech LTD, with which the Bank has concluded an agreement for the technical provision of Remote Identification (Video Identification and Photo Identification)**.**

ICT Service Provider No. 2 – Dokobit, UAB, with which the Bank has concluded an agreement for the use of a Qualified Electronic Signature by Clients. The ICT Service Provider may redirect the Identifiable Person to its cooperation partner or a group company for the issuance of a Qualified Electronic Signature, if the Identifiable Person wishes to obtain such a Qualified Electronic Signature.

Instruction – The User Cabinet (Remote Identification) User Manual.

Legal Arrangement – an arrangement that is not a legal person but has independent legal capacity and capacity to act, and which may include a founder, an authorized person, a supervisor (administrator), or equivalent roles, and a beneficial owner – if no natural person benefiting from the arrangement has been identified, the person in whose interest the legal arrangement has been established or operates, or any other natural person who ultimately exercises control over the legal arrangement through ownership or other means. For the purposes of these Rules and their implementation, a Legal Arrangement registered in a Public Register shall be treated as a legal person.

Client – a natural or legal person to whom the Bank provides or intends to provide banking services.

Client's Representative – a natural person who represents a legal person by operation of law (e.g., a member of the management board).

Timestamp – an electronically signed confirmation that an electronic document has

been marked at a specific date and time by a certification service provider.
User Cabinet – an information and communication technology system maintained by the Bank, which allows a new Client/Client's Representative to communicate remotely with the Bank and submit documents.
Remote Identification – a method of identification whereby the Client is identified remotely, without being physically present, using information and communication technology solutions – Video Identification or Photo Identification.
Non-resident – a natural or legal person who, according to the Rules, is not a Resident, as well as foreign diplomatic, consular, international organization, and other representations in the Republic of Latvia.
Rules – these General Terms and Conditions for Remote Client Identification of the Bank, binding upon the Parties.
Operator – a Bank employee who performs the Video Identification of the Client / Client's Representative.
Beneficial Owner – a natural person who is the owner of the Client – a legal person or a Legal Arrangement – or who exercises control over the Client, or on whose behalf, for whose benefit, or in whose interest a business relationship is established or an occasional transaction is carried out. A Beneficial Owner is at least:

a) in relation to legal persons – a natural person who owns, directly or indirectly, more than 25 percent of the share capital or voting rights of the legal person, or otherwise exercises control over it, directly or indirectly;

b) in relation to Legal Arrangements – a natural person who owns, or in whose interest the Legal Arrangement has been established or operates, or who exercises control over it, directly or indirectly, including any person acting as the founder, trustee (administrator), protector (if any), beneficiary, or – where no individual beneficiaries have yet been determined – the group of persons in whose interest the Legal Arrangement is established or operates, as well as any other natural person who ultimately exercises control over the Legal Arrangement, directly or indirectly.

Identification Document(s) – documents verifying the identity of a Client/Client's Representative (passport or identity card).
Applicable Law – the laws and regulations in force in the Republic of Latvia, as well as legal acts issued by the Bank of Latvia and the Cabinet of Ministers, which are binding upon the Bank and the Client.
Politically Exposed Person (PEP) – a person who holds or has held a prominent public function in the Republic of Latvia, another EU Member State, or a third country, including: a senior official of the state; head of an administrative unit (municipality); head of government; minister (deputy minister or assistant deputy minister, if such position exists in the relevant country); state secretary or other senior official in the government or an administrative unit (municipality); member of parliament or equivalent legislative body; member of a governing body of a political party; judge of a constitutional court, supreme court, or another high-level judicial body; member of the board or council of the supreme audit institution; member of the board or council of a central bank; ambassador, chargé d'affaires; senior officer in the armed forces; member of the board or council of a state-owned enterprise; or a director, deputy

director, member of the board, or person holding an equivalent position in an international organization.

Family Member of a Politically Exposed Person – a person who is related to a Politically Exposed Person as:

a) a spouse or a person equivalent to a spouse. A person is considered equivalent to a spouse only if such status is recognized by the laws of the relevant country;
b) a child of the PEP or of the PEP's spouse or equivalent, and the child's spouse or equivalent;
c) a parent;
d) a sibling.

Public Registers – registers granted public credibility status by law and used for obtaining publicly credible information (e.g., the Register of Enterprises of the Republic of Latvia, Register of Invalid Documents, etc.), as well as equivalent foreign registers.

Parties – the Client and the Bank, as referred to in these Rules.

Resident –

a) a natural person who is a citizen or non-citizen of the Republic of Latvia, or a stateless person, refugee, or person granted alternative status, and who holds one of the identity documents specified in the Law on Identity Documents;
b) a legal person, including a foreign entity, that is registered and operates in the Republic of Latvia, as well as diplomatic, consular, or other official representations of the Republic of Latvia abroad.

GTC – the Bank's General Terms and Conditions, binding upon the Parties. (Note: "VDN" has been translated as "GTC – General Terms and Conditions". If your bank uses another official abbreviation, this can be adapted.)

Video Identification – identification of a person via video streaming in compliance with the requirements of the Applicable Law.

1. Application of the Terms

1.1. These Rules govern the legal relationship between the Client and the Bank with respect to Remote Identification.
1.2. The General Terms and Conditions (GTC) are binding upon the Client to the extent that these Rules do not provide otherwise.
1.3. In relation to Remote Identification, the Client must additionally comply with the Instruction.
1.4. The Terms, the Price list, the Manual, and the GTS are available to the Client on the Bank's website (www.magnetiqbank.com).
1.5. Unless specified otherwise in the Terms, terms and words used in the singular also apply to the plural of such terms or words, and vice versa.
1.6. The headings of sections of the Terms are intended for convenience only and should not be used in the interpretation of the Terms.
1.7. In the event of contradiction or confusion between the wording of the Terms in Latvian and in a foreign language, the wording in Latvian shall prevail.
1.8. The Terms have been divided into sections, clauses and subclauses. Section headings are provided for reference only and do not regulate the relationship between the Bank and the Client, but are meant only to assist in navigating the Terms. Subclauses apply in combination with relevant clauses only.
1.9. In communication, the Bank and the Client use a mutually intelligible language (Latvian, English or Russian).

1.10. The operations of the Bank is supervised by the Bank of Latvia.

2. Amendments to the Terms

2.1. The Bank is entitled to amend the Terms unilaterally and without prior notice.
2.2. The publication of amendments to the Terms is governed by the same provisions as those stated in the GTS regarding the publication of amendments to the GTS.
2.3. Once amendments of the Terms come into force, they are deemed to be an integral part of the Terms.
2.4. In any event of amendment of the Terms, the Bank, within the term specified in the Terms, will publish relevant information on the Bank's website, www.magnetiqbank.com.
2.5. The Client is obliged to keep track of information regarding amendments to the Terms on the Bank's website, www.magnetiqbank.com.

3. General Requirements for Remote Identification

3.1. A person wishing to become a Client of the Bank remotely must first submit the documents specified in Annex 1 and identity documents (of the Client, the Client's Representative, and the Beneficial Owner) and undergo Remote Identification of the Client / Client's Representative.
3.2. The Client / Client's Representative must upload to the User Cabinet and use for Remote Identification identity documents that permit entry into the Republic of Latvia (for example, a foreign passport, if such document is issued by the relevant country).
3.3. Copies of any identity documents, as well as other documents required to be submitted in the User Cabinet pursuant to these Rules, must bear the holder's signature (a physical signature—applicable only for the Beneficial Owner—or a Secure Electronic Signature), a printed name, and an indication of the place and date of signing, along with the statement "Copy submitted to AS Magnetiq Bank." This information may also be provided in English or Russian.
3.4. The conclusion of the agreement is governed by the General Terms and Conditions (GTC), in compliance with these Rules.
3.5. The Bank performs Remote Identification only in respect of legal persons registered in the Public Register (including Legal Arrangements registered in the Public Register) and adult natural persons, both Residents and Non-Residents, unless otherwise provided by Applicable Law.
3.6. Remote Identification applies both to new Clients and to existing Clients (for example, when changes to the composition of the board of directors are required, identity document data need to be updated, or amendments to Bank-determined contract terms are necessary).
3.7. Remote Identification takes place in several stages, including: 1) registration in the User Cabinet and two-factor authentication; 2) signing documents with a Secure Electronic Signature or using the service provided by ICT Service Provider No. 2 if the Client / Client's Representative does not have a Secure Electronic Signature, and submitting them via the User Cabinet; 3) making a cashless transfer (payment of commission fees) from the Client's account with another payment service provider; 4) conducting due diligence on the Client / Client's Representative;5) performing Remote Identification of the Client / Client's Representative in the information technology system of ICT Service Provider No. 1.
3.8. For new Clients remotely identified, if the Bank decides to commence cooperation with the Client, all Bank services will be available, except for:

3.8.1. basic account;
3.8.2. capital deposit account.

3.9. The Bank reserves the right not to provide any other Bank services if it considers that in-person identification is necessary for the respective Client/Client's Representative to receive the service.

3.10. Only the Operator has the right to perform the Client's/Client's Representative's Video Identification. The Bank confirms that the person performing the Video Identification is an employee authorized to carry out Video Identification on behalf of the Bank. The Bank sends a link to the Client's/Client's Representative's specified e-mail address, through which the Client/Client's Representative is redirected to the ICT Service Provider No. 1 system to perform Video Identification.

3.11. For Video Identification, the Client/Client's Representative must ensure a stable and uninterrupted internet connection with sufficient capacity for Video Identification, a computer with a camera and microphone/mobile phone, and identity documents.

3.12. Before Remote Identification of a new Client is performed, the Client must obtain access (register) to the User Cabinet and submit the documents specified in Annex 1 and identity documents (of the Client, Client's Representative, Beneficial Owner).

3.13. Before Remote Identification of an existing Client – in case of a legal person, the Client's Representative must obtain access (register) to the User Cabinet and submit the documents specified in clauses 5.1.2 and 5.1.3 of these Rules.

3.14. Clients/Client's Representatives must comply with the same requirements concerning the User Cabinet as the Client must comply with regarding Internet Banking according to these Rules and the General Terms and Conditions (GTC).

3.15. The technical support for the Remote Identification process is provided by ICT Service Provider No. 1.

3.16. The requirements for Photo Identification are set out in Section 6 of the Rules.

3.17. The requirements for Video Identification are set out in Section 7 of the Rules.

3.18. The Bank may refuse to perform the Client's/Client's Representative's Remote Identification or require in-person identification by sending a notification via e-mail and SMS if:

3.18.1. circumstances indicating that Remote Identification does not correspond to the Client's/Client's Representative's inherent risk of money laundering and terrorism and proliferation financing are detected;

3.18.2. circumstances indicating insufficient security, appropriateness, or truthfulness of the information obtained during the Remote Identification process are detected;

3.18.3. inconsistencies with the information obtained during the Client's/Client's Representative's due diligence are detected.

3.19. The Bank does not perform Remote Identification in the following cases:

3.19.1. The Client exhibits any characteristics of a shell entity;

3.19.2. The Client is a Legal Arrangement/legal person not registered in the Public Register;

3.19.3. The Client wishes to open an account through an authorized person.

3.20. The Bank or the Identified Person (Client/Client's Representative) may terminate any stage of the Remote Identification process at any time without providing reasons.

3.21. In the case of a Client who is a legal person, Remote Identification is carried out only for those Client's Representatives who are intended to represent the Client in relations with the Bank.

3.22. The Bank has the right to request any other additional information and/or documents. The Client is obliged to submit all information/documents requested by the Bank within the prescribed deadlines.
3.23. The Client is responsible for the truthfulness, accuracy, completeness, and timeliness of all information, data, and documents provided to the Bank. The Client shall indemnify the Bank for any losses incurred due to late, false, forged, or incomplete submission of information/documents.
3.24. The Bank is entitled to request original documents or notarized copies with notarized translations into Latvian, Russian, or English, as well as legalized or apostilled documents according to the procedure prescribed by Applicable Law.
3.25. If the Client fails to comply with the Bank's request to submit necessary documents and/or provide information within the Bank's specified deadline, the Bank has the right to refrain from performing and approving Remote Identification until the necessary documents and/or information are received.
3.26. All requests, notices, and warnings issued by the Bank to the Client through the User Cabinet or e-mail have the legal force of documents signed by an authorized representative of the Bank.
3.27. Notifications and information are exchanged between the Parties as follows:
3.27.1. The Client sends to the Bank electronically via the User Cabinet;
3.27.2. The Bank sends to the Client at its discretion electronically via the User Cabinet or e-mail;
3.27.3. In urgent cases, such as security threats or unforeseen technical problems, communication is conducted by phone or any other promptly available means.
3.28. For the avoidance of doubt, any dispatch is deemed received:
3.28.1. if sent via the User Cabinet – on the next day following the day the relevant information was submitted to the recipient in the User Cabinet;
3.28.2. if sent by e-mail – on the day the receipt of electronically signed messages is confirmed according to Applicable Law.
3.29. The Client pays the Bank fees (commissions) for document review and Remote Identification in the amount and manner specified in the Price List and the Rules. The Bank has the right to withhold the Bank's fees (commissions) according to the procedure specified in the Rules and GTC.
3.30. The Bank requires the Client to pay the fees (commissions) specified in the Price List. The Bank has the right to require payment of fees (commissions) by cashless transfer from another payment service provider. The Bank may impose other restrictions regarding commission payment.
3.31. The Bank informs the Client via the User Cabinet about the amount and payment procedure of the Bank's commission for document review and Remote Identification, and if necessary, about the payment of other Bank commissions in accordance with the Price List. In case of a change of the Client's representative, the Bank has the right to deduct the commission from funds available in the Client's account.
3.32. If the Client has not paid the Bank the due commissions in full, the Bank has the right not to perform document review and Remote Identification without notifying the Client or compensating any losses, and to cancel access to the User Cabinet as specified in Section 5. The Bank has the right to request payment of commissions specified in the Price List before providing the relevant Bank service.
3.33. The Bank is not obliged to accept a representation document in which the powers of representation are not clearly and unambiguously formulated or if the Bank doubts the validity or authenticity of the representation document.

3.34. The Client/Client's Representative being identified is informed that personal data, including facial biometric data, will be processed during Remote Identification to perform unique identification of the natural person. Remote Identification and data processing are carried out in compliance with the Cabinet Regulation No. 392 of 3 July 2018 "Procedure for the remote identification of clients by subjects of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing."
3.35. Personal data processing in the Bank is performed in accordance with Applicable Law and the Bank's Data Subject Notice on personal data processing (formerly Personal Data Processing Policy), which is available on the Bank's website – www.magnetiqbank.com.
3.36. The Bank verifies the information submitted by the Client/Client's Representative in Public Registers and closed databases to verify the accuracy of the information provided, assess the Client's risk level, presence on sanction lists, lists of Politically Exposed Persons, their family members, or persons closely associated with Politically Exposed Persons, and to evaluate the possibility of providing the Client with selected Bank services.
3.37. Information obtained during Remote Identification is processed by the Bank in accordance with these Rules, the GTC, the Bank's Data Subject Notice on personal data processing, and Applicable Law.
3.38. The Parties agree that any dispute, disagreement, or claim arising from these Rules concerning their violation, termination, or invalidity will be resolved in accordance with the provisions of the GTC.

4. Registration of new Clients in the User Cabinet and access to means of authentication

4.1. The provisions of this section apply to new Clients.
4.2. To gain access to the User Cabinet, the Client fills out a registration form on the Bank's website https://onboarding.magnetiqbank.com/, providing the following information:
4.2.1. For a natural person – mobile phone number, email address, citizenship country (maximum two), marks confirming that they have read the Bank's Notice to Data Subjects on Personal Data Processing, the Price List, and have read and undertake to comply with the Terms and Conditions, Rules, and Instructions, and chooses and confirms a password for access to the User Cabinet;
4.2.2. For a legal entity – the Client's representative's mobile phone number, email address, country of registration of the legal entity, marks confirming that they have read the Bank's Notice to Data Subjects on Personal Data Processing, the Price List, and have read and undertake to comply with the Terms and Conditions, Rules, and Instructions, and chooses and confirms a password for access to the User Cabinet.
4.3. After entering the registration data, the Client will receive an email verification code at the provided email address and an SMS verification code on the mobile phone number provided.
4.4. To create access to the User Cabinet, the Client enters the received codes into the Bank's registration form. Upon successful registration, an identification device (the provided mobile phone number) is linked to the Client/Client's representative at the Bank, which will be used for Client/Client representative authentication going forward.
4.5. To log into the User Cabinet for the first time after registration, the Client (natural person) or Client's representative uses the email address or the provided mobile phone number (as the login name) and the password selected during registration.

4.6. Access to the User Cabinet is granted only to an Identifiable person in the case of a natural person, or a person providing information on behalf of the Client in the case of a legal entity who completed the registration pursuant to clause 4.2.2.
4.7. The User Cabinet allows a new Client to communicate with the Bank, submit and receive documents, and receive instructions regarding the identification process.
4.8. After logging into the User Cabinet, the Identifiable person (natural person) or the person providing information on behalf of the Client (legal entity) selects the desired services.
4.9. After selecting the desired services, if the Client is a natural person, they provide: first name, last name, personal identification number/date of birth, and preferred communication language; attach at least one identity document for each citizenship held (if multiple citizenships); and attach documents required for Client due diligence according to Annex 1 of the Rules.
4.9.1. If “Additional payment card user” or “Internet banking user” was selected among the services, additionally:
4.9.2. Provide information about the associated Client;
4.9.3. Attach at least one identity document for each citizenship held (if multiple citizenships).
4.10. After selecting the desired services, the Client’s representative (for a legal entity) provides:
4.10.1. About the Client – country of registration, company name, registration number, registration date, industry sector, company website URL, number of employees, and preferred communication language;
4.10.2. About the Beneficial Owner (PLG) – first name, last name, date of birth, personal identification number, citizenship, ownership share, tax residence country;
4.10.3. About the Client’s representative – first name, last name, date of birth, personal identification number, citizenship, position and form of representation (solely or jointly with other authorized signatories), email address, and indication whether the representative will act on behalf of the Client at the Bank;
4.10.4. bout the owner (natural person) – first name, last name, date of birth, personal identification number, citizenship, country of residence, ownership share;
4.10.5. About the owner (legal entity) – country of registration, company name, registration number, registration date, ownership share;
4.10.6. About the person providing information on behalf of the Client – first name, last name, date of birth, personal identification number, role in the company.
4.10.7. Attach at least one identity document for each citizenship held (if multiple citizenships);
4.10.8. Attach documents required for Client due diligence according to Annex 1 of the Rules.
4.11. After providing the information, the Client or Client’s representative submits the initial information to the Bank in accordance with clauses 4.9 or 4.11, necessary for assessing the Client’s eligibility. Submission of the initial information is done by pressing the “Submit” button, which confirms that the submitted documents/information are accurate, complete, and truthful.
4.12. Identifiable persons must successfully pass Photo Identification.
4.13. Upon successful Photo Identification, the Identifiable person (natural person) or the person providing information on behalf of the Client (legal entity) fills in and submits the necessary documents to the Bank. The documents required depend on the services of interest to the Client or Client’s representative.
4.14. If the documents received in the User Cabinet are deemed correctly completed, the Bank will request them to be:

4.14.1. Signed with a Secure Electronic Signature (if the Client/Client's representative has one) and submitted in the User Cabinet, or

4.14.2. Use the service provided by ICT Service Provider No. 2 (if the Client/Client's representative does not have a Secure Electronic Signature). The signing with a Secure Electronic Signature and the possibility to obtain such a signature is provided by ICT Service Provider No. 2. If the Client/Client's representative uses this option, the Bank will attach the Document Package and other documents (in PDF format) in the User Cabinet and initiate the process so that the Client/Client's representative can receive a link for signing and/or obtaining the signature.

4.15. If the Client's representative at the Bank has indicated a representation scope together with another Client representative(s), the documents must be signed according to the specified representation scope (i.e., signed together by two, three, etc.).

4.16. If the Client's representatives (in the required representation scope) do not have Secure Electronic Signatures, the documents must be signed with a secure electronic signature provided by ICT Service Provider No. 2, according to the specified representation scope (i.e., signed together by two, three, etc.). In this case, the Bank sends a link via email to the relevant Client representatives to the ICT Service Provider No. 2 system. The Client representatives, using the link received by email, access the ICT Service Provider No. 2 information technology system and, by following the instructions, sign the documents.

4.17. Receipt of documents and remote identification by the Bank does not yet constitute a decision to start cooperation with the Client. The decision made will be communicated to the Client by email.

5. Change of Client's Representative at the Bank (for a legal entity) for an existing Client

5.1. A new Client's representative must create a User Account. The new Client's representative initially:

5.1.1. registers and logs into the User Account in accordance with Section 4;

5.1.2. uploads a document confirming the new Client's representative's authority to represent the Client – the legal entity;

5.1.3. uploads at least one identity document for each citizenship (if there are multiple citizenships);

5.1.4. completes and signs with a Secure Electronic Signature or uses the service provided by ICT Service Provider No. 2;

5.1.5. completes Photo Identification in accordance with Section 6.

5.2. If the documents received in the User Account are deemed to be properly completed, the Bank will request that they be signed with a Secure Electronic Signature and submitted through the User Account, in accordance with points 4.14.–4.16.

6. Photo Identification

6.1. This section applies to both new and existing Clients, e-commerce service clients who wish to submit changes in the composition of the Client's representatives at the Bank (e.g., a new board member), as well as Additional Payment Card users who wish to receive an Additional Payment Card, and Internet Banking users.

6.2. Before starting the Photo Identification, an email with a link will be sent to the Identifiable Person through the User Cabinet, which redirects them to the IT Service Provider No.1 system.

6.3. After logging into the IT Service Provider No.1 system, the Identifiable Person will undergo Photo Identification according to the requirements of this section.

6.4. During the Photo Identification process, the Identifiable Person performs the following actions:

6.4.1. Upon request from the IT Service Provider No.1 system and following its instructions, take photos of the Identifiable Person's identity document;

6.4.2. Upon request from the IT Service Provider No.1 system and following its instructions, record a short video file (liveness check).

6.5. If the Photo Identification process is interrupted, the Identifiable Person has the opportunity to repeat the Photo Identification using the same link.

7. Video Identification

7.1. This section applies to both new Clients and existing Clients who wish to update documents (for example, submit changes in the composition of the Client's representatives at the Bank or renew financial terms), as well as existing Clients who wish to remove operational restrictions, Additional Payment Card users who want to receive an Additional Payment Card, and Additional Internet Banking users.

7.2. The identity document used by the Client/Client's representative at the time of Video Identification must be valid for at least 5 working days after the completion of the Video Identification and must be the same document previously submitted to the Bank via the User Cabinet.

7.3. If the Bank recognizes Video Identification as a suitable identification method for the respective Client/Client's representative, then before the Video Identification starts, a notification with a link will be sent via email. Through this link, the Client/Client's representative will be redirected to the IT Service Provider No.1 system. The Client/Client's representative must log into the IT Service Provider No.1 system at the specified time, enter the mobile phone number registered with the Bank, enter the code received on the mobile phone, review and accept the terms of use of the IT Service Provider No.1 system, and perform the Video Identification according to the instructions provided by the Operator.

7.4. During Video Identification of the Client/Client's Representative, the Operator has the right to:

7.4.1. to inform the Client/Client's Representative about the progress of the Video Identification process and about making a recording;

7.4.2. to ask the person being identified to ensure that they are alone in the room. In the event of technical issues, with the Operator's consent, the Client/Client's Representative may rely on the assistance of a third party to remedy technical issues, who must leave the room after remedying the issues;

7.4.3. to ask the Client/Client's Representative to ensure that their head and shoulders are in plain sight, their face is not in a shadow and is clearly distinguishable from the background and from other objects, no filters are in use, the face is not covered, the documents being presented are clearly legible;

7.4.4. to request presentation of the Identification Document at various angles;

7.4.5. to take a photo of the Client/Client's Representative;

7.4.6. to take a photo of the Identification Document of the Client/Client's Representative;

7.4.7. to make a video recording;

7.4.8. to ask questions;

7.4.9. to terminate Video Identification:

7.4.9.1. if in doubt whether the Client/Client's Representative is alone in the room;

7.4.9.2. if there are technical issues (e.g., poor audibility or video streaming disruptions);

7.4.9.3. if in doubt whether the Client/Client's Representative is under the influence of alcohol, toxic, narcotic or psychotropic substances (e.g., the person being identified is unable to answer questions, behaves in an inappropriate/undignified manner, uses swear words etc.);

7.4.9.4. if the Client/Client's Representative's head or shoulders are not in plain sight, their face is in a shadow and/or not clearly distinguishable from the background and other objects, filters are in use, the face is covered, the documents being presented are not clearly legible etc.;

7.4.9.5. if prohibited under the Terms or the Applicable Legislation.

7.4.10. to perform other activities necessary for fulfilling the requirements of Video Identification.

7.5. The IT service provider No.1 has the right to record the IP address of the internet connection of the Client and/or the Client's representative.

7.6. If the Video Identification process was interrupted for the Client/Client's representative, then after resolving the cause of the interruption (e.g., fixing technical issues), the Client/Client's representative must perform the Video Identification again by logging into the IT service provider No.1 system (using the same link) and repeating the actions specified in clause 7.3.

7.7. If the Video Identification process was unsuccessful for the Client/Client's representative (an appropriate notification is displayed on the screen), the Client/Client's representative must perform the Video Identification again by logging into the IT service provider's system (using the same link) and repeating the actions specified in clause 7.3. Before redoing the Video Identification, the Client/Client's representative must ensure that the identity document complies with the requirements of clause 3.2 and that its validity period meets the requirements of clause 7.2.

7.8. The Bank is entitled to require the Client/Client's Representative to undergo repeated Video Identification at any time by giving the Client/Client's Representative notice via e-mail and SMS.

7.9. The Bank is entitled to unilaterally determine the maximum allowed number of attempts to perform Video Identification if the process of Video Identification is interrupted.