ANTI-MONEY LAUNDERING POLICY
TeleTrade - DJ International Consulting Ltd
June 2019/

POLITICA PRIVIND COMBATEREA SPĂLĂRII BANILOR
TeleTrade - DJ International Consulting Ltd
Iunie 2019

1. Scope of the policy Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature or the origin of funds derived from the illegal activities. Money laundering involves not only the proceeds of drugs trafficking, but funds related to other illegal activities, including fraud, corruption, organized crime, terrorism and many other crimes. Generally the money laundering consists of three stages: • Placement: introduction of cash originating from illegal / criminal activities into financial or non-financial institutions. • Layering: separating the proceeds of criminal activities form their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity. • Integration: placing the laundered proceeds back into the economy in such a way that they re – enter the financial system as apparently legitimate funds. This Policy is developed and periodically updated by the Risk Management/Compliance and AntiMoney Laundering Officer of TeleTrade - DJ International Consulting Ltd (the Company) based on the general principles set up by the Board of Directors of the Company in relation to the prevention of money laundering and terrorist financing. The Policy applies to all employees of the Company and aims to setup key roles and responsibilities for the staff members as well as to ensure compliance with the following legislation: • THE PREVENTION AND SUPPRESSION OF MONEY LAUNDERING AND TERRORIST FINANCING LAWS No. 188(I)/2007 of 2007-2018 (the Law) • DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing • DIRECTIVE DI144-2007-08 OF 2012, DIRECTIVE	**1. Domeniul de aplicare al politicii** Spălarea banilor reprezintă participarea la orice tranzacție care încearcă să ascundă sau să tăinuiască natura sau originea fondurilor provenite din activitățile ilegale. Spălarea banilor implică nu numai veniturile provenite din traficul de droguri, ci și fondurile legate de alte activități ilegale, inclusiv fraudă, corupție, crimă organizată, terorism și multe alte infracțiuni. În general, spălarea banilor presupune trei etape: •Plasare: introducerea banilor proveniți din activități ilegale/criminale în activități financiare sau de altă natură în instituții non-financiare. • Acordarea de fonduri: separarea veniturilor din activități criminale de la sursa lor prin utilizarea straturilor de tranzacții financiare complexe. Aceste straturi sunt concepute pentru a împiedica traseul de audit, pentru a ascunde originea fondurilor și de a oferi anonimatul. • Integrare: plasarea banilor spălați înapoi în economie în așa fel încât aceștia să fie reintroduși în sistemul financiar drept fonduri aparent legitime. Această Politică este dezvoltată și actualizată periodic de către Directorul de Management al Riscului/Ofițer pentru combaterea spălării banilor al companiei TeleTrade - DJ International Consulting Ltd (Compania) pe baza principiilor generale stabilite de Consiliul de Administrație al Companiei în ceea ce privește prevenirea și combaterea spălării banilor și finanțarea terorismului. Politica se aplică tuturor angajaților Companiei și urmărește stabilirea rolurilor cheie și a responsabilităților pentru membrii personalului, precum și asigurarea conformității cu următoarea legislație: • PREVENIREA ȘI SUSPENDAREA SPĂLĂRII BANILOR ȘI A FINANȚĂRII TERORISMULUI LEGILE nr. 188 (I)/2007 din 2007-2018 (Legea) • DIRECTIVA (UE) 2015/849 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopuri financiare de spălare a banilor sau finanțării terorismului • DIRECTIVA D144-2007-08 DIN 2012, DIRECTIVA DI144-2007-08 (A) DIN 2016 SI DIRECTIVA

DI144-2007-08(A) OF 2016 AND DIRECTIVE DI144-2007-08(B) OF 2016 OF THE CYPRUS SECURITIES AND EXCHANGE COMMISSION FOR THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING (the AML Directive) • Any other Directives, Circulars and Guidelines issued by the Cyprus Securities and Exchange Commission (CySEC), the Unit of Combating Money Laundering (MOKAS) and any other authority entrusted with the task of combating Money Laundering The Company has established principles and procedures to prevent money laundering and combat terrorism financing, in accordance with the risk profile of its products, services, clients and geographic locations. All amendments and/or changes of current version of the Policy must be approved by the Company's Board of Directors.	DI144-2007-08 (B) DIN 2016 A CYPRUS SECURITIES AND EXCHANGE COMMISSION PENTRU PREVENIREA SPĂLĂRII BANILOR ȘI A FINANȚĂRII TERORISMULUI (Directiva AML) • Orice alte directive, circulare și instrucțiuni emise de Cyprus Securities and Exchange Commission (CySEC), Unit of Combating Money Laundering (MOKAS) și orice altă autoritate însărcinată cu combaterea spălării banilor. Compania a stabilit principii și proceduri pentru prevenirea spălării banilor și combaterea finanțării terorismului, în conformitate cu profilul de risc al produselor, serviciilor, clienților și locațiilor sale geografice. Toate modificările și/sau modificările versiunii curente a politicii trebuie să fie aprobate de către Consiliul de Administrație al Companiei.
2. Clients' acceptance policy Inadequate understanding of the client's profile and purpose of investment activity may expose the Company to a number of risks. In order to minimize such risks, the Company has developed the Client Acceptance Policy.	**2. Politica de acceptare a clienților** O înțelegere incorectă a profilului clientului și a scopului activității investiționale poate expune compania la o serie de riscuri. Pentru a minimiza astfel de riscuri, compania a elaborat Politica de Acceptare a Clientului.
3. Risk-based approach The Company applies appropriate measures and procedures, on a risk based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing ppears to be higher. This approach will enable the Company to assign to its clients the following risk categories: • High risk clients • Medium risk clients • Low risk categories	**3. Abordarea bazată pe risc** Compania aplică măsurile și procedurile adecvate, pe baza unei abordări bazate pe risc, astfel încât să își concentrează eforturile în acele zone în care riscul de spălare a banilor și finanțare a terorismului se dovedește a fi mai ridicat. Această abordare va permite companiei să atribuie clienților săi următorul risc categorii: • Clienți cu risc ridicat • Clienți cu risc mediu • Categorii de risc scăzut
4. Dynamic Risk Management Risk Management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Client's activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.	**4. Managementul riscului dinamic** Managementul riscului este un proces continuu, realizat dinamic. Evaluarea riscului nu este un eveniment izolat cu o durată limitată. Activitățile clientului se schimbă, precum și serviciile și instrumentele financiare furnizate de societate. Același lucru se întâmplă și cu instrumentele financiare și cu tranzacțiile utilizate pentru spălarea banilor sau finanțarea terorismului.
5. Know Your Client Procedures The prime method for preventing money	**5. Cunoașteți procedurile de client** Principala metodă de prevenire a spălării banilor

laundering is by carrying out “Know Your Client” procedures. With thorough knowledge of clients, counterparties and the origin of client’s funds, unusual or suspicious behaviour can be identified, including false identities, unusual transactions, changing behaviour or other indicators where laundering may be occurring. The Company ensures that the clients’ identification records remain completely updated with all relevant identification data and information throughout the business relationship. The Company examines and checks, on a regular basis, the validity and adequacy of the clients’ identification data and information it maintains, especially those concerning high risk clients.	este realizarea "Know Your Client Procedures" (Cunoașteți procedurile de client "). Cu o cunoaștere aprofundată a clienților, a contrapartidelor și a originii fondurilor clientului, pot fi identificate comportamente neobișnuite sau suspecte, inclusiv identități false, tranzacții neobișnuite, schimbări de comportament sau alți indicatori în care poate apărea. Compania asigură că înregistrările de identificare ale clienților rămân complet actualizate, cu toate datele și informațiile relevante de identificare pe parcursul relației de afaceri. Compania examinează și verifică în mod regulat validitatea și adecvarea datelor de identificare ale clienților și a informațiilor pe care le întreține, în special cele referitoare la clienții cu risc ridicat.
5.1. Establishment of Identification for Individual Customers The identity will be established to the Company’s satisfaction by reference to official identity papers or such other evidence as may be appropriate under the circumstances including, without limitation: -full name; date of birth; origin; marital status; name of wife/husband, if married; name of parents; -complete address, including phone number and city code; occupation; information on the earnings and his/her financial situation. Identification documents must be valid at the time of the establishment of the business relationship. Evidence of the potential client’s identity should be in the form of a true copy or a copy of: a) Passport or National ID card if the potential client does not have a passport b) Proof of residence - this document can be in the form of a utility bill (electricity, water or landline telephone bill, home internet bill), local authority tax bill, a confirmation letter issued by the municipality, bank statement or other equivalent document showing the potential client’s full name (cannot be wife/ husband/ other family member’s name) and should be dated within the last 6 months. Provided that there is a reasonable explanation, a proof of residence issued in the name of the potential client’s parent (mother/father) or spouse can be accepted, however,	**5.1. Stabilirea identității pentru clienți individuali** Identitatea va fi stabilită în funcție de satisfacția Companiei prin referire la fișe de identitate oficiale sau alte dovezi care ar putea fi adecvate în circumstanțe, incluzând, fără limitare: -Numele complet; Data de nastere; origine; starea civilă; numele soției / soțului, dacă este căsătorit; numele părinților; - adresa completă, inclusiv numărul de telefon și codul orașului; ocupaţie; informații privind câștigurile și situația financiară a acestuia. Documentele de identificare trebuie să fie valabile în momentul stabilirii relației de afaceri. Dovada identității clientului potențial ar trebui să fie sub forma unei copii corecte sau a unei copii a următoarelor documente: a) pașaport sau carte de identitate națională dacă potențialul client nu are pașaport b) Dovada de ședere - acest document poate fi sub formă de factură de utilitate (electricitate, apă, factură telefonică la domiciliu, factură de internet la domiciliu), factură fiscală de la autoritățile locale, scrisoare de confirmare emisă de municipalitate, declarație bancară sau alt document echivalent care să prezinte numele complet al potențialului client (nu poate fi numele soției/soțului să fie date în ultimele 6 luni. Cu condiția să existe o explicație rezonabilă, o dovadă de reședință emisă în numele potențialul client al părintelui (mamă/tată) sau soț/soție poate fi acceptat, cu toate acestea, documente suplimentare pentru stabilirea

additional documents to establish the relationship, such as, birth certificate, marriage certificate, should be received. Depending on the country of origin the Company may request additional documents and will be considered on a case by case basis following a risk based approach by the AMLCO and directors. The Company applies enhanced customer identification and due diligence procedures in respect of the clients that pose a high level of risk for money laundering or terrorist financing and are classified by the Company as high risk according to Clients Acceptance Policy. The Company will follow the following measures in order to verify the identity of non face to face clients: 1) Where possible, direct and personal contact with the potential client is established. The staff member of the Company or its remote organizational units, who has met with the client in person and verified his identity, confirms a face to face meeting in the client's profile in the CRM software; 2) Telephone contact with the client at his residence or office, before the establishment of a business relationship or the occasional transaction, on a telephone number which has been provided by the potential client; 3) Contact with the client through email at an email address provided by the potential client. The Company may also apply the following additional verification methods: a) The first payment of the operations is carried out through an account opened in the customer's name with a credit institution operating and licensed in a Member State or in a third country, which imposes requirements on combating money laundering equivalent to those of the EU Directive; b) Video Call with the potential client. It is provided that a potential customer, whose identity was verified hereunder cannot deposit an amount over €2.000 per annum, irrespective of the number of accounts that he keeps with the Company, unless an additional measure as per above paragraph is taken in order to verify his identity. In such case the Company monitors both the amount of the client's deposit and the risk for money	relației, cum ar fi certificatul de naștere, certificat de căsătorie. În funcție de țara de origine, Compania poate solicita documente suplimentare și va fi luată în considerare de la caz la caz, în urma unei abordări bazate pe riscuri a AMLCO și a directorilor. Compania aplică proceduri îmbunătățite de identificare a clienților și de due diligence în ceea ce privește clienții care prezintă un nivel ridicat de risc pentru spălarea banilor sau finanțarea terorismului și sunt clasificați de către Companie ca risc ridicat în conformitate cu Politica de Acceptare a Clienților. Compania va urma urmatoarele măsuri pentru a verifica identitatea persoanei în lipsa acesteia: 1) Atunci când este posibil, se stabilește un contact direct și personal cu potențialul client. Angajatul Companiei sau a unităților sale organizaționale la distanță, care s-a întâlnit cu clientul în persoană și-a confirmat identitatea, confirmă o întâlnire reală cu clientul în profilul lui din CRM; 2) contactul telefonic cu clientul la domiciliul sau biroul său, înainte de stabilirea unei relații de afaceri sau a unei tranzacții ocazionale, pe un număr de telefon care a fost furnizat de potențialul client; 3) Contact cu clientul prin e-mail la o adresă de e-mail furnizată de acesta. Compania poate aplica, de asemenea, următoarele metode suplimentare de verificare: a) Prima plată a operațiunilor se efectuează printr-un cont deschis în umele clientului cu o instituție de credit care operează și care deține o licență într-un stat membru sau în țara terță, care impune cerințe privind combaterea spălării banilor echivalente cu directivele UE; b) Apel video cu potențialul client. Se prevede că un potențial client, a cărui identitate a fost verificată în temeiul prezentului articol, nu poate depune o sumă de peste 2 000 EUR pe an, indiferent din numărul de conturi pe care le are la companie, cu excepția cazului în care se iau măsuri adiționale conform paragrafului de mai sus pentru a-i verifica identitatea. În acest caz Compania monitorizează atât valoarea depozitului clientului, cât și riscul de spălare a banilor sau de finanțare a terorismului, avertizează clientul în mod adecvat și în timp util pentru procedura de mai sus pentru a obține

laundering or terrorist financing, as well warns the client appropriately and in due time
for the above procedure in order to obtain the client's express consent prior to its commencement.;
c) Requiring for identification documents to be provided in the form of certified true copies of the originals. Certification can be made by:
• a third party, such as, accountant or a lawyer, provided that additional measures/procedures are applied as per the paragraph **Reliance on third parties for client identification and due diligence purposes** of this Policy;
• a competent authority or person that, pursuant to the relevant provisions of the laws of their country, is responsible to certify the authenticity of documents or information.

6. Reporting of Suspicious Transactions to MOKAS

Suspicious transactions are transactions or other activities that have no apparent lawful purpose or is not the sort in which a particular client would normally be expected to engage in, and the Company knows of no reasonable explanation for the transaction or activity after examining the available facts, including the background and possible purpose of the transaction or activity. The
Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the AMLCO its suspicion to MOKAS.

7. Record Keeping
The Company must maintain records of:
• Client identification documents obtained
• Any additional documents/information obtained during the relationship
• All World-Check and Accuity World Compliance Reports performed for the client, as well as all results for the screening on sanctions' lists
Details of all relevant business transactions carried out
for clients for a period of seven years after the end of the business relationship with their customer

consimțământul expres al clientului înainte de a-și exprima acordul;
c) Solicitarea ca documentele de identificare să fie furnizate sub formă de copii certificate conforme cu originalul. Certificarea poate fi făcută de:
• o terță parte, cum ar fi contabilul sau un avocat, cu condiția aplicării unor măsuri/proceduri suplimentare conform paragrafului **Sprijinul pe terțe persoane în vederea identificării clientului și diligența acestei politici**;
• o autoritate competentă sau o persoană care, conform prevederilor relevante ale legilor țării lor, este responsabilă pentru a certifica autenticitatea documentelor sau a informațiilor.

6. Raportarea tranzacțiilor suspecte către MOKAS
Tranzacțiile suspecte sunt acele tranzacții sau alte activități care nu au un scop legal sau nu sunt acelea în care se așteaptă în mod normal să le desfășoare clientul, iar Compania nu cunoaște explicații rezonabile pentru tranzacție sau activitate după examinarea faptelor disponibile, inclusiv contextul și scopul posibil al tranzacției sau al activității.
Compania, în cazurile în care există o încercare de a executa tranzacții care sunt suspecte că sunt legate de spălarea banilor sau finanțarea terorismului, raportează, prin intermediul AMLCO, suspiciunea sa față de MOKAS.

7. Păstrarea înregistrărilor
Compania trebuie să țină evidența următoarelor acte:
• Documentele de identificare a clientului obținute
• Toate documentele/informațiile suplimentare obținute în timpul relației
• Toate rapoartele de conformitate World-Check și Accuity World Compliance Reports efectuate pentru client, precum și toate rezultatele pentru examinarea listelor de sancțiuni. Detalii privind toate tranzacțiile de afaceri relevante efectuate pentru clienți, pentru o perioadă de șapte ani de la încheierea relației de afaceri cu clientul sau după data unei tranzacții ocazionale.
Aceste informații pot fi folosite ca dovadă în orice anchetă ulterioară a autorităților.

or after the date of an occasional transaction. This information may be used as evidence in any subsequent investigation by the authorities. The records kept provide audit trail evidence during any subsequent investigation. In practice, the business units of the Company will be routinely making records of work carried out for clients in the course of normal business and these records should be archived.	înregistrările păstrate dovezi ale traseului de audit în timpul oricărei investigații ulterioare. În practică, unitățile de afaceri ale Companiei vor face în mod obișnuit înregistrări ale lucrărilor efectuate pentru clienți în cursul activității obișnuite, iar aceste înregistrări ar trebui arhivate.