

**How to cite this article:**

Sedaghati, A., Farahbaksh, M., & Sadeghi Ziazi, H. (2025). Executive Methods Applied under Anti-Money Laundering Laws and Regulations in the Iranian Legal System. *Journal of Historical Research, Law and Policy*, 3(1), 1-18. <https://doi.org/10.61838/jhrp.441>



Article history:
Original Research

Dates:

Submission Date: 12 September 2024

Revision Date: 03 February 2025

Acceptance Date: 12 February 2025

Publication Date: 01 March 2025

Executive Methods Applied under Anti-Money Laundering Laws and Regulations in the Iranian Legal System

1. Alireza. Sedaghati¹ : Ph.D. Student, Department of Criminal Law and Criminology, Emirates Branch, Islamic Azad University, Emirates, Iran
2. Mojtaba. Farahbaksh^{2*}: Assistant Professor, Department of Law, Shahid University, Tehran, Iran
3. Hatam. Sadeghi Ziazi³: Associate Professor, Department of Law, Payame Noor University, Tehran, Iran

*corresponding author's email: mfarahbaksh@shahed.ac.ir

ABSTRACT

Money laundering, as a complex process, involves the processing of proceeds derived from criminal activities for the purpose of concealing or disguising the illicit origin of funds and comprises three stages: placement, layering, and integration. The present dissertation constitutes fundamental and theoretical research and employs a descriptive-analytical method based on available books, scholarly articles, authoritative legal sources, laws and regulations concerning money laundering, as well as the anti-money laundering regulations applicable to executive bodies, institutions, and persons involved in matters relating to money laundering. The purpose of this study is to examine and elucidate Iran's executive policy toward combating the crime of money laundering. Iran has acceded to several conventions concerning the combating of money laundering and corruption, and a number of effective measures have been undertaken in this regard. These include the adoption of the 2019 Anti-Money Laundering Executive Regulation, through which significant executive measures have been introduced, particularly measures that are substantially aligned with the recommendations of the Financial Action Task Force (FATF). Such measures include the accurate and comprehensive identification of clients; the establishment of the Financial Intelligence Unit referred to in Article 7 of the Anti-Money Laundering Act; the establishment of an anti-money laundering unit within each relevant executive body; the imposition of obligations on covered persons to ensure the effective combating of money laundering; and particular attention to designated non-financial businesses and professions, as well as the obligations imposed on covered persons and operators of non-financial businesses and professions in combating money laundering. Nevertheless, despite these developments, Iran's executive criminal policy still lacks sufficient effectiveness and efficiency in ensuring an effective response to money laundering.

Keywords: Money Laundering, Executive Criminal Policy, Iran, Combating Corruption, Financial Action Task Force (FATF).

Introduction

Although the existence of a foreign-exchange control regime and the difficulty of transferring foreign currency through lawful channels diminish the attractiveness of Iran's banking system for money-laundering purposes, several factors have made Iran a suitable environment for money-laundering activities. These factors include Iran's proximity to some of the world's largest drug-producing countries; its location along transit routes for lawful and unlawful goods, particularly narcotic drugs produced in the Golden Triangle and Golden Crescent and transported



to Europe; its proximity to regional free-trade centers such as Dubai and Bahrain; the extensive length of its land and maritime borders and, consequently, its considerable vulnerability to organized smuggling of goods and human beings; its adjacency to the newly independent Central Asian states affected by mafia-type criminal structures; its proximity to Iraq, as one of the principal centers of regional crisis, and to Turkey, as a country facing substantial levels of criminal activity; the expansion of drug-related offenses within the country; the growth of property crimes, bribery, and administrative corruption; the expansion of commodity smuggling; the growth of the informal sector of the economy; and, particularly, underdevelopment, economic disorder, and structural weaknesses in the foundations of the economy (1). One of the most important obligations imposed on Member States by United Nations conventions is therefore the adoption of appropriate proactive and reactive measures to combat offenses relating to financial and administrative corruption, including money laundering. In the Iranian legal system, in addition to numerous measures adopted to counter the offense of money laundering, various governmental and judicial institutions have incorporated the fight against money laundering among their principal objectives and duties. Under domestic regulations, namely the Anti-Money Laundering Act and its Executive Regulation, various methods have been prescribed for detecting money laundering and identifying offenders. Accordingly, the present study, employing a descriptive-analytical research method and taking into account Iran's particular circumstances, examines Iran's executive criminal policy for combating money laundering. With respect to customer identification and the retention of identity and transactional records, it should be noted that customer identification and the retention of identity and transactional records do not, at the initial stage, have a direct relationship with crime detection. Nevertheless, during prosecution and investigation, they facilitate the identification of the suspect, and at the stage of proving the offense, they facilitate identification of the offender, because conducting financial transactions without leaving any trace of the perpetrator makes attribution of the conduct to a particular person difficult. Furthermore, customer identification, in addition to facilitating identification of the perpetrator, may also have a preventive effect. In other words, when a person knows that all of his or her activities are recorded and traceable, that person will exercise greater caution in his or her conduct. It can therefore be argued that recording such activities increases, to some extent, the risk associated with committing an offense and consequently reduces the likelihood of criminal conduct. This method, however, will be effective only where it is impossible, or at least severely restricted, to carry out such activities outside the regulated environment. Otherwise, where these activities can readily be conducted outside the regulated sphere, preventive measures will not only be ineffective but may also cause capital to leave the formal economy and move into the informal sector. Recommendation 10 of the Financial Action Task Force (FATF), under the heading "Customer Due Diligence," provides: "Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. Financial institutions should be required to undertake customer due diligence measures when: (1) establishing business relations; (2) carrying out occasional transactions: (a) above the applicable designated threshold (USD/EUR 15,000); or (b) wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16; (3) there is a suspicion of money laundering or terrorist financing; or (4) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data." The principle that "financial institutions must conduct adequate customer due diligence" should be incorporated into national legislation. Each country may determine, through legislation or enforceable instruments, how the specific customer due diligence obligations are to be established. Measures required for adequate customer due diligence include: (a) identifying the customer and verifying the customer's identity using reliable, independent source documents, data, or information; (b) identifying

the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner so that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements, this should include financial institutions understanding the ownership and control structure of the customer; (c) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and (d) conducting ongoing due diligence on the business relationship and scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds. Financial institutions should be required to apply each of the customer due diligence measures set out in paragraphs (a) to (d) above; however, the extent of such measures should be determined on a risk-sensitive basis in accordance with the Interpretive Notes to this Recommendation and Recommendation 1. Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the establishment of a business relationship or while conducting transactions for occasional customers. Where money-laundering and terrorist-financing risks are effectively managed and where interruption of the normal conduct of business is essential, countries may permit financial institutions to complete verification as soon as reasonably practicable following the establishment of the relationship. Where financial institutions are unable to comply with the requirements set out in paragraphs (a) to (d), subject to appropriate modification of the extent of the measures according to a risk-based approach, they should be required not to open the account, commence the business relationship, or perform the transaction; or they should terminate the business relationship with existing customers and consider filing a suspicious transaction report in relation to the customer. These requirements should apply to all new customers, although financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk and should conduct due diligence on such existing relationships at appropriate times" (1). The Anti-Money Laundering Act and its Executive Regulation have adopted several measures in this regard. These measures concerning customer identification and the retention of customers' identity and transactional records are examined separately below.

Customer Identification

Customer identification necessarily involves at least two parties: first, the natural or legal person who, pursuant to applicable regulations, is authorized or required to carry out identification; and second, the customer. Anti-money laundering regulations address both aspects and carefully define or enumerate the relevant persons. The term "customer" is not defined in the Act; however, Paragraph 11 of Article 1 of the 2019 Executive Regulation provides: "Customer: any natural or legal person, whether acting as principal, attorney, or legal representative, who approaches a covered person in order to obtain services or privileges, conduct a transaction, transfer property, obtain financing, or carry out any financial or economic activity." The 2018 amended Anti-Money Laundering Act, in identifying those subject to customer-identification obligations, provides in Article 7: "Persons, institutions, and bodies subject to this Act (as referred to in Articles 5 and 6), depending on the nature of their activities and organizational structure, shall comply with the following requirements: (a) verification of the identity and identification of customers and beneficial owners and, where action is taken through a representative or attorney, verification of the status and identity of the representative or attorney and the principal. Note: The provisions of this paragraph shall not negate the necessity of identity verification under other laws and regulations." This Article concerns covered persons required to verify customers' identities, and the phrase "institutions and bodies" is redundant

because such entities are themselves included within the legal concept of persons. As stated in this Article, covered persons are specified in Articles 5 and 6 of the Act. Article 5 provides: “All owners of non-financial businesses and professions and non-profit institutions, as well as natural and legal persons whose inclusion within the scope of the Act requires express reference to their names, such as the National Iranian Oil Company, the Industrial Development and Renovation Organization of Iran, and others, shall implement the executive regulations adopted by the Council of Ministers in connection with this Act and the Counter-Terrorist Financing Act.” Article 6 further provides: “All persons referred to in Article 5 of this Act shall, upon the request of the Council or the Financial Intelligence Center, provide them with information required for implementation of this Act, as approved by the Council of Ministers.” Paragraph 33 of Article 1 of the Executive Regulation defines “identification” as follows: “The process of obtaining and continuously reviewing customer information relating to identity verification and assessment of money-laundering and terrorist-financing risk. Levels of identification comprise three levels: simplified, standard, and enhanced.” Under this classification, depending on the required level, three forms of customer due diligence—simplified, standard, and enhanced—are prescribed. In this regard, Article 51 of the 2019 Executive Regulation provides: “Covered persons shall, for purposes of implementing identification procedures, classify the risk arising from their business interactions with customers in accordance with anti-money laundering and counter-terrorist financing regulations and shall implement identification procedures proportionate to such risk at the three levels of simplified, standard, and enhanced due diligence. In addition, policies, guidelines, and procedures for customer identification shall be based on a risk-based approach so as to establish continuous and targeted monitoring of customer business relationships, and the level of information obtained from customers, including information concerning the beneficial owners of legal persons, shall be determined, retained, and updated in proportion to the customer’s risk.” Article 52 of the 2019 Executive Regulation further provides: “Financial and credit institutions and exchange offices shall organize appropriate customer-identification processes and procedures—including simplified, standard, and enhanced identification—in such a manner that, while sufficient information is obtained at the commencement of the business relationship, and throughout its duration, it is possible to assess the risk associated with establishing a relationship with the customer and to adopt identification procedures proportionate to that risk.”

Simplified Customer Due Diligence

Article 53 of the 2019 Executive Regulation of the Anti-Money Laundering Act defines simplified due diligence as follows: “Covered persons may, after conducting a comprehensive risk assessment, limit themselves to simplified identification procedures. In other cases, the implementation of standard or enhanced identification procedures in accordance with the provisions of this Regulation shall be mandatory.” Under simplified due diligence, certain measures must be adopted. These measures are specified in Article 54 of the Regulation as follows: “For purposes of implementing simplified identification procedures, covered persons shall adopt less stringent customer-identification measures proportionate to the customer’s level of risk. Such measures shall not contravene other anti-money laundering and counter-terrorist financing regulations.” Some of these measures include: (1) reducing the frequency with which customer-identification information is updated; (2) reducing the extent of ongoing monitoring and scrutiny of transactions on the basis of the customer’s expected level of activity; and (3) refraining from collecting detailed information or taking specific measures to understand the intended purpose and nature of business relationships where that purpose and nature can be inferred from the type of transactions or established

business relationships. Pursuant to Note 2 to Article 52 of the Executive Regulation, the provision of non-basic services below the prescribed threshold does not require assessment of the risk of establishing a business relationship with the customer.

Simplified Customer Due Diligence for Natural Persons

The information required is specified in Note 1 to Article 52 of the Executive Regulation: “The required information shall, at a minimum, include matters such as the type of person (natural or legal), the customer’s nationality, the geographical area of residence and legal domicile, the expected origin and destination of the customer’s transactions and operations, occupation and nature of activity, level of income and sources of assets, services requested by or provided to the customer, the purpose of opening an account or establishing a business relationship, direct or intermediary use of received services, and the use or receipt of services on a non-face-to-face basis, so as to determine the nature, purpose, and risk of the business relationship with the customer.” Article 55 of the Regulation provides: “Covered persons shall, when providing any business interaction, even below the prescribed threshold, including any receipt or payment, transfer of funds, issuance and payment of checks, extension of credit facilities, issuance of different types of debit and payment cards, issuance of various guarantees, purchase and sale of foreign currency, certificates of deposit and participation securities, acceptance of guarantees and guarantors’ obligations in any form such as signing promissory notes, bills of exchange, and documentary credits, purchase and sale of shares, provision of various insurance services, leasing services, purchase of investment securities, provision of various tax services including preparation and completion of tax returns and maintenance of statutory books, and provision of various services by non-governmental public institutions, implement the customer identity-verification process, whether the customer is permanent or occasional and whether a natural or legal person, and record the relevant information in their registers or information systems. Such action shall be taken before establishing a business relationship, providing any product or service, or conducting any transaction.” Article 56 of the Regulation further provides: “Covered persons shall, for purposes of implementing the customer identity-verification process, obtain the customer’s identity information and verify the conformity of such information with valid identification documents.” Pursuant to the Notes to this Article, where a person acts on behalf of a principal, covered persons shall, in addition to verifying the representative’s identity, obtain valid and official documents evidencing the representation, such as a power of attorney. Under Note 3 to Article 56, valid identification documents for natural persons are determined and announced by the Financial Intelligence Center.

Simplified Customer Due Diligence for Legal Persons

The information required is specified in Note 1 to Article 52 of the Executive Regulation: “The required information shall, at a minimum, include matters such as the type of person (natural or legal), the customer’s nationality, the geographical area of residence and legal domicile, the expected origin and destination of the customer’s transactions and operations, occupation and nature of activity, level of income and sources of assets, services requested by or provided to the customer, the purpose of opening an account or establishing a business relationship, direct or intermediary use of received services, and the use or receipt of services on a non-face-to-face basis, so as to determine the nature, purpose, and risk of the business relationship with the customer.” Article 56 of the Regulation further provides: “Covered persons shall, for purposes of implementing the customer identity-verification process, obtain the customer’s identity information and verify the conformity of such information with

valid identification documents.” Pursuant to the Notes to this Article, where a person acts on behalf of a principal, covered persons shall, in addition to verifying the representative’s identity, obtain valid and official documents evidencing the representation, such as a power of attorney. Under Note 3 to Article 56, valid identification documents for legal persons are determined and announced by the Financial Intelligence Center. Article 57 of the Regulation provides: “With respect to legal persons in the process of formation, financial and credit institutions may open an account without obtaining a national identification number, provided that they obtain an official introduction letter from the State Organization for Registration of Deeds and Properties and block withdrawals from that account until the national identification number is obtained.”

Standard Customer Due Diligence

Pursuant to Article 58 of the 2019 Executive Regulation: “Financial and credit institutions and exchange offices shall implement standard identification procedures in the following circumstances: (1) prior to providing basic services; (2) prior to providing non-basic services and establishing a business relationship with an occasional customer in relation to transactions exceeding the prescribed threshold, regardless of whether the transaction is conducted as a single transaction or as several linked transactions; (3) prior to international electronic transfers; (4) where there is suspicion of money laundering or terrorist financing; (5) where there are doubts regarding the accuracy or adequacy of information previously obtained from the customer; and (6) where there are grounds indicating a change in the customer’s circumstances or information during monitoring and supervision procedures.” Updating information under standard due-diligence procedures shall not take longer than one year (Note to Article 58). The measures that covered persons shall adopt for standard due diligence are specified in Article 59 of the 2019 Executive Regulation as follows: (1) verifying the identity of the customer solely by means of reliable and independent sources and obtaining valid documents; (2) ensuring identification of the beneficial owner on the basis of reliable information and documentation; (3) understanding the nature, purpose, and extent of the customer’s activities during establishment of the business relationship; (4) reviewing supporting documents of persons who, in any capacity—including executor, guardian, custodian, attorney, or representative of a legal person—approach financial and credit institutions on behalf of others, in addition to conducting identity-verification procedures in respect of such persons; (5) implementing standard due diligence on an ongoing basis through appropriate measures such as ensuring that information obtained from the customer is up to date, continuously monitoring the customer according to the customer’s expected level of activity, and comparing the customer’s transactions with information obtained from the customer; and (6) collecting and retaining information concerning assessment of the risk arising from business relationships.

Standard Customer Due Diligence for Natural Persons

Pursuant to Article 60 of the 2019 Executive Regulation, financial and credit institutions, for purposes of implementing standard identification procedures in relation to natural persons, shall observe the following minimum measures and obtain, as appropriate, three general categories of information—identity information, economic information, and beneficial-ownership information—together with valid supporting documentation from the customer or relevant authorities. After verifying the correctness and authenticity of the information, they shall maintain it electronically in the customer’s profile. The minimum identity, economic, and beneficial-ownership information concerning natural persons is as follows: (1) verification of the customer’s identity and collection of identity

information, including first name, surname, year of birth, national identification number, father's name, living status and, where deceased, date of death, and the postal code of the place of residence, through valid identification documents; (2) taking appropriate measures, such as obtaining a written declaration and an undertaking as to the truthfulness of the declaration, to determine whether the customer is acting on his or her own behalf or on behalf of other beneficial owners and, where a beneficial owner exists, obtaining the beneficial owner's identity information in accordance with this Article; and (3) economic information, including employment information, such as particulars of the employer, organization, or institution of employment in the case of employees and workers, and occupational title and business-license number in the case of self-employed persons; estimated annual income; estimated aggregate annual deposits to and withdrawals from the account; estimated maximum amount of each transaction; information on other sources of income, such as the securities-exchange trading code and the tracking code of real-estate lease agreements; the statutory inspector's and auditor's reports; the tax return; and the economic identification code, where applicable. Pursuant to Note 2 to Article 60, the identity, economic, and beneficial-ownership information required for foreign natural persons is as follows: (1) verification of the customer's identity and collection of identity information, including first name and surname, father's name, grandfather's name, special identification number, date and place of birth, living status and date of death, residence status, date of entry into the country, postal code of place of residence, type and validity period of identification documents, and nationality, through valid identification documents; (2) taking appropriate measures, such as obtaining a written declaration and an undertaking as to the truthfulness of the declaration, to determine whether the customer acts on his or her own behalf or on behalf of other beneficial owners and, where a beneficial owner exists, obtaining the beneficial owner's identity information in accordance with this Article; and (3) economic information, including employment information and the activity permit obtained from the Ministry of Cooperatives, Labour and Social Welfare, such as particulars of the employer, organization, or institution of employment in the case of employees and workers, and occupational title and business-license number in the case of self-employed persons; estimated annual income; estimated aggregate annual deposits and withdrawals; estimated maximum amount of each transaction; information on other sources of income, such as the securities-exchange trading code and the tracking code of real-estate lease agreements; the statutory inspector's and auditor's reports, where the customer is legally required to have an inspector or statutory auditor; the tax return; and the economic identification code, where applicable.

Standard Customer Due Diligence for Legal Persons

Article 61 of the 2019 Executive Regulation provides with respect to identification of legal persons: "Financial and credit institutions shall, for purposes of implementing standard identification procedures in relation to legal persons, observe the following minimum measures and obtain, as appropriate, three general categories of information—identity information, economic information, and beneficial-ownership information—as specified in this Article, together with valid documents, from the customer or the relevant authorities. After verifying the correctness and authenticity of the information, they shall maintain the information and supporting documentation electronically in the customer's profile. (1) Verification of the customer's identity and collection of the following identity information through supporting documentation: (a) national identification number, name of the legal person, type of legal person (commercial or non-commercial; for-profit or non-profit; governmental or non-governmental; and, in the case of commercial companies, the type of company, such as limited liability company, public joint-stock company, private joint-stock company, etc.), registering authority (including the Companies and Non-Commercial Institutions

Registration Office, Ministry of Interior, etc.), date of establishment, status (including active, dissolved, or liquidation completed), and date of dissolution/completion of liquidation, based on valid documents evidencing the existence of the legal person, such as its articles of association and company agreement; (b) the ownership structure and control structure of the customer, including information on major shareholders, members of the board of directors, senior executive managers, and, where applicable, inspectors or auditors, based on the regulations governing and supervising the legal person; and (c) the verified address and postal code of the legal domicile of the head office and principal place of business, based on valid documents evidencing the existence of the legal person. (2) Identification of the beneficial owner of legal persons by obtaining identity information concerning the following persons: (a) natural persons or those legal persons that directly or indirectly hold at least a 25% ownership interest or one managerial seat on the board of directors of the legal person shall be deemed beneficial owners; (b) persons who exercise control over legal persons through other instruments, such as a power of attorney, where there is doubt regarding paragraph (a) or where no natural person exercises control through ownership; and (c) senior managers of the legal person where neither paragraph (a) nor paragraph (b) applies. (3) Understanding the subject matter, nature, and extent of the customer's activity by obtaining information such as the field of activity, for example manufacturing or commercial activities; estimated sources of income, such as investment income and proceeds from product sales; estimated sales, costs, and income; estimated volume of exports and imports; estimated annual account turnover; and estimated number of annual transactions, based on valid documents including the legal person's business license, most recent tax return, or one of the reports attached to financial statements that can be verified through the Iranian Association of Certified Public Accountants."

Enhanced Customer Due Diligence

Pursuant to Article 77 of the 2019 Executive Regulation of the Anti-Money Laundering Act, concerning enhanced customer identification, covered persons are required to adopt enhanced identification procedures and measures where the risk associated with the business relationship is assessed as high. Note 1 provides that financial and credit institutions shall, at a minimum, implement enhanced due-diligence procedures in the following cases: (1) business relationships with natural and legal persons, including financial and credit institutions, whose risk is identified as higher according to international authorities and after approval by the Supreme National Security Council; (2) cases where the beneficiary of a life-insurance policy is a legal person or the beneficiary of a legal arrangement; (3) foreign correspondent accounts; (4) provision of private-banking services; (5) provision of basic services to politically exposed persons; and (6) unusual transactions or unusual transaction patterns that have no apparent lawful or economic purpose. Pursuant to Article 78 of the Regulation, where covered persons, on the basis of available information or reasonable evidence and indications, suspect that the identity of a person or entity corresponds to a freezing list, they shall implement enhanced due-diligence procedures in relation to that person or entity. Where such identity correspondence is confirmed by the anti-money laundering unit or the highest responsible authority of the covered person, the rules concerning freezing of the person's assets shall be applied in accordance with this Regulation. The minimum measures to be adopted by covered persons under enhanced due-diligence procedures, pursuant to Article 79 of the Regulation, are as follows: (1) obtaining additional information concerning the customer, such as economic activities and volume of assets, and updating the customer's profile, including beneficial-ownership information, at shorter intervals; (2) obtaining additional information concerning the nature of the business relationship; (3) obtaining information on the source of capital or

source of the customer's assets; (4) obtaining information concerning the reasons for high-value transactions; (5) obtaining approval from senior management for commencement and continuation of the business relationship; (6) conducting inquiries through required information systems or comprehensive databases; (7) increasing the level of scrutiny in supervision and monitoring by increasing control points, increasing the frequency of obtaining and reviewing information concerning the business relationship, and identifying transaction patterns requiring further scrutiny; and (8) commencing service provision through a newly opened account only after funds have been transferred from an account in the customer's name at a bank that applies acceptable standard due-diligence requirements. Where implementation of enhanced due-diligence procedures is not possible, covered persons shall refrain from providing services to the customer (Note 3 to Article 80 of the Regulation).

Retention of Identity and Transaction Records

Recommendation 11 of the Financial Action Task Force, under the heading "Record-Keeping," provides: "Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions, including the amounts and types of currency involved, where applicable, so as to provide, if necessary, evidence for prosecution of criminal activity. Financial institutions should be required to keep all records obtained through customer due diligence measures—for example, copies or records of official identification documents such as passports, identity cards, driving licenses, or similar documents—account files and business correspondence, including the results of any analysis undertaken, such as inquiries to establish the background and purpose of complex, unusual, and large transactions, for at least five years after the business relationship has ended or after the date of an occasional transaction. Financial institutions should be required by law to maintain records concerning transactions and information obtained through customer due diligence. Customer due diligence information and transaction records should be made available to domestic competent authorities upon appropriate authority."

Retention of identity and transactional records is, in fact, complementary to customer identification, because identification constitutes a measure designed to ensure that, where verification of a person's identity becomes necessary in the future, the relevant identification records can be consulted and the required information retrieved. This, in turn, requires retention of such records. Accordingly, the legislature established specific rules on this matter in the 2019 Anti-Money Laundering Executive Regulation. As to the scope of record retention, Paragraph (d) of the Note to Article 7 of the Anti-Money Laundering Act provides: "Records relating to identification of the customer and owner, account records, and records of domestic and foreign operations and transactions shall be retained for at least five years after termination of the business relationship or completion of an occasional transaction, in accordance with procedures to be determined by the Executive Regulation of this Act. Note: This paragraph shall not prejudice other laws requiring retention of documents for a period exceeding the aforementioned period." Chapter Eleven of the 2019 Executive Regulation of the Anti-Money Laundering Act is entitled "Retention of Records and Information." Concerning the retention period, Article 142 provides: "Covered persons shall retain documents, records, and evidence relating to business relationships for ten years in such a manner that, upon request by competent authorities, they can be provided without delay." Moreover, pursuant to the Note to Article 142: "Where a covered legal person is dissolved, the documents, records, and information shall be retained by the liquidation office or liquidation board for ten years." As to the types of records subject to retention, Article 142 of the Regulation

provides: (1) documents, evidence, and records relating to customer-identification procedures, whether simplified, standard, or enhanced, including copies of documents proving the identity of the customer and beneficial owner; (2) documents, evidence, and records relating to accounts and business correspondence; and (3) documents, evidence, and records relating to financial transactions and operations, whether domestic or international, in such a manner that such records contain sufficient information concerning the assets, including the amounts and, where applicable, the types of currency used in each transaction, and make it possible to reconstruct the process of each transaction and provide the information, documentation, and evidence necessary for criminal prosecution. Regarding ease of retrieval, Article 143 of the Regulation provides: "Covered persons shall record and retain information, records, and documents in such a manner that, if requested by the Center or competent authorities, including special law-enforcement officers, the information contained in such documents shall be accessible within two working days. In addition, the originals of documents and records shall, upon request by the Center or other competent authorities, be provided within one week." Pursuant to Note 1 to this Article, responsibility for providing information and documents rests with the covered natural person in the case of natural persons and with the highest-ranking authority of the covered person in the case of legal persons. Note 2 to the same Article further provides that such information and documents must make it possible to reconstruct the chain of transactions where necessary (2).

Mandatory Reporting

One of the common methods of laundering illicit proceeds is the use of the banking system, financial and credit institutions, and notary offices. Consequently, focusing on these institutions and establishing mechanisms for detecting such activities within them can make a significant contribution to combating money laundering. Most countries, including Iran, have therefore established a "reporting" regime for this purpose. Recommendation 9 of the Financial Action Task Force, under the heading "Financial Institution Secrecy Laws," provides: "Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations." Chapter Ten of the 2019 Executive Regulation of the Anti-Money Laundering Act is devoted to "Reporting." Under these provisions, reporting relates either to transactions exceeding the prescribed threshold or to suspicious transactions and operations.

Reporting Transactions Exceeding the Prescribed Threshold

Article 139 of the Executive Regulation of the Anti-Money Laundering Act provides: "Employees working under the authority of covered persons shall record all business interactions exceeding the prescribed threshold, whether individual or aggregated, including transactions, transfers of funds, and transactions in which the customer makes daily cash payments, and shall report them, together with the customer's explanations as confirmed by the customer, to the anti-money laundering units. Such units shall submit a summary of the relevant forms at the end of each week in the manner prescribed by the Center and shall retain the originals under fully secure conditions." Article 141 of the Regulation further provides: "All natural and legal persons may, where they become suspicious of the commission of money laundering or terrorist financing, report the matter directly to the Center." Pursuant to Paragraph 13 of Article 1 of the Regulation, the "prescribed threshold" means: "The threshold amount stipulated in the Public Procurement Act for small-value transactions, whether in cash or its equivalent in other currencies or precious commodities, as annually approved by the Council of Ministers pursuant to Note 1 to Article 3 of the Public

Procurement Act.” This mechanism may be abused in practice, as persons seeking to launder money may conduct transactions and investments below the prescribed threshold or divide large amounts into smaller amounts and have them deposited or invested through other persons, such as children, employees, or similar persons, in banks and investment institutions. These deficiencies necessitate a complementary mechanism. Accordingly, the Anti-Money Laundering Act and its Executive Regulation also provide for the reporting of suspicious transactions and operations.

Reporting Suspicious Transactions and Operations

Article 7 of the 2018 amended Anti-Money Laundering Act, concerning the reporting of transactions suspected of involving money laundering, provides: “Persons, institutions, and bodies subject to this Act, as referred to in Articles 5 and 6, shall, according to the nature of their activity and organizational structure, comply with the following requirements: ... (c) submission to the Financial Intelligence Center of reports concerning transactions or operations, or attempted operations, exceeding the amount approved by the Council, as well as suspicious banking, registration, investment, foreign-exchange, brokerage, and similar transactions and operations.” Note 2 to Article 7 of the Anti-Money Laundering Act defines suspicious transactions and operations as any transaction, receipt or payment of property, whether physical or electronic, or an attempt thereto, that would, in light of circumstances such as its value, subject matter, or parties, ordinarily give rise to suspicion that an offense has occurred. Examples include: (1) financial transactions and operations relating to a customer that are manifestly inconsistent with and substantially exceed the customer’s expected level of activity; (2) discovery of forgery, false statements, or misrepresentation by customers before or after a financial transaction or operation is conducted, as well as at the time of obtaining basic services; (3) financial transactions and operations that are found, in any manner, to be fictitious or nominal and in which the true owner is another person; (4) financial transactions and operations where the legal domicile of any party is located in a high-risk area from the perspective of money laundering, with the list of such areas to be determined by the Council; and (5) financial transactions and operations exceeding the threshold prescribed in the Executive Regulation, even where customers withdraw from conducting the transaction or operation before or during its performance, or terminate the contract after completion without a logical justification. Persons, institutions, and bodies subject to Articles 5 and 6 of the Anti-Money Laundering Act shall, upon observing transactions or operations suspected of money laundering or terrorist financing, immediately and without notifying the customer report the matter to the anti-money laundering unit of the relevant body. The anti-money laundering unit of the covered person shall submit suspicious transaction reports to the Center, through the system established by the Center for collection of suspicious transaction reports, no later than the end of the same working day (Article 135 of the Regulation and Note 1 thereto). Financial and credit institutions shall establish appropriate criteria for identifying suspicious transactions at different organizational levels, including branches and supervisory offices, and shall communicate such criteria to those levels following approval by the Center. Article 137 of the Regulation provides: “Covered persons shall, in addition to the reviews conducted during service provision or transaction execution for the purpose of identifying suspicious transactions and operations, identify such suspicious transactions and operations by matching information against data contained in the covered person’s databases.” FATF Recommendations also address the obligation to report suspicious transactions. Recommendation 20 of the Financial Action Task Force, under the heading “Reporting of Suspicious Transactions,” provides: “If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity or are

related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit.” Recommendation 23 of the Financial Action Task Force, under the heading “Designated Non-Financial Businesses and Professions: Other Measures,” further provides: “The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions, subject to the following qualifications: (a) lawyers, notaries, other independent legal professionals, and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to other professional activities of accountants, including auditing; (b) dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold; and (c) trust and company service providers should be required to report suspicious transactions when, on behalf of or for a client, they engage in a transaction in relation to the activities described in paragraph (e) of Recommendation 22.” Finally, reporting entities must be protected from adverse consequences resulting from disclosure of confidential information and must also be prohibited from disclosing information to any authority other than the financial intelligence unit. Recommendation 21 of the Financial Action Task Force, under the heading “Tipping-Off and Confidentiality,” provides that financial institutions and their directors, senior officers, and employees shall: “(a) be protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by legislative, regulatory, or administrative provision, if they report their suspicions in good faith to the financial intelligence unit, even if they did not know precisely what the underlying criminal activity was and regardless of whether illegal activity actually occurred; and (b) be prohibited by law from disclosing the fact that a suspicious transaction report or related information is being filed with the financial intelligence unit.” With regard to the consequences of disclosing confidential information and filing reports, Note 1 to Article 136 of the Executive Regulation provides that suspicious transaction reports and other reports that covered persons are required to submit shall not give rise to any accusation or liability against good-faith reporters implementing the law and this Regulation, nor shall such reports constitute an accusation against the persons who are the subject of the report, and their submission to the Center shall not constitute disclosure of personal secrets. However, disclosure of collected information and documents, or direct or indirect use thereof for the benefit of oneself or another person by government officials or other persons specified in the Anti-Money Laundering Act, is prohibited, and a violator shall be sentenced to a Grade Five discretionary imprisonment (Article 8 of the Anti-Money Laundering Act).

National Cooperation and Coordination

For the purpose of establishing effective communication and cooperation among governmental bodies, executive agencies, ministries, and organizations, Chapter Three of the Executive Regulation of the Anti-Money Laundering Act provides several mechanisms aimed at effective and efficient combating of money laundering. Article 16 of the Regulation requires the National Organization for Civil Registration to establish an integrated database of identity information concerning Iranian natural and legal persons in such a manner that covered persons can obtain, online and without restriction, the latest basic identity information and information concerning associated persons. Changes in basic identity information and lists of invalidated identification codes, or, in the case of legal persons, dissolution and completion of liquidation, as well as suspended identification codes, shall be made available to covered persons on a daily basis. The Ministry of Health and the Legal Medicine Organization are likewise required

to provide the necessary information online to the National Organization for Civil Registration (Articles 16 and 20 of the Regulation and their Notes). In addition, pursuant to Article 25 of the Regulation, the State Organization for Registration of Deeds and Properties shall establish an integrated database of official powers of attorney in such a manner that covered persons can at all times verify their status online. The Ministry of Information and Communications Technology shall establish a geolocation-based unique-address system for natural and legal persons in such a manner that, in addition to standardizing addresses, it enables covered persons, for purposes of anti-money laundering and counter-terrorist financing regulations, to verify and display the geographical location on a map. The Ministry shall also establish a national mobile-phone-number system and provide the necessary infrastructure for assigning one mobile telephone number to every natural or legal person, whether Iranian or foreign, and shall make unrestricted online verification available to covered persons (Articles 17 and 22 of the Regulation). The Ministry of Industry, Mine and Trade is required to enable electronic registration, through the Comprehensive Trade System, of transactions involving gold, precious metals and stones, and antiques, as well as transactions involving automobiles and high-value carpets. Once electronic registration becomes available, allocation or replacement of vehicle license plates by the Law Enforcement Force may occur only after verification through this system and confirmation that the vehicle transaction has been registered (Articles 18 and 19 and their Notes). Furthermore, the Ministry of Industry, Mine and Trade, in cooperation with the State Organization for Registration of Deeds and Properties, is required to establish a geolocation-based national real-estate transaction registration system in such a manner that all natural and legal persons can register transactions involving immovable property, whether supported by official or unofficial instruments. All owners of immovable property supported by unofficial documents shall, within six months following implementation of the system, upload supporting documents evidencing their transactions to that system (Article 23 and its Note). The Ministry of Intelligence shall establish an integrated identity-information database for foreign natural and legal persons in such a manner that covered persons can at all times and without restriction verify online the latest basic identity information, addresses, and associated persons (Article 21 of the Regulation). The Law Enforcement Force shall establish an integrated database containing information on the entry and exit of natural persons across the country's borders in such a manner that the Center and special law-enforcement officers can, on a daily basis, verify the status of individuals' presence within the country, including lists of foreign nationals whose authorized period of stay has expired (Article 24 of the Regulation). The Ministry of Cooperatives, Labour and Social Welfare shall establish an integrated employment-information database for natural persons, both Iranian and foreign, in such a manner that covered persons can at all times verify their latest employment status. In cooperation with the Iranian National Tax Administration, the Ministry shall identify employment relationships among persons in such a manner that the Center and the Central Bank can at all times verify the employment-related associates of specified persons (Article 26 of the Regulation). The Iranian National Tax Administration shall, at three-month intervals, make available to covered persons all tax returns of natural and legal persons and the latest status of taxpayers' tax files. It shall also use information from the integrated employment-information database referred to in Article 26 of the Regulation, pursuant to Paragraph (e) of Article 169 of the Direct Taxation Act, as tax indicators for assessment of taxpayers' tax liabilities. Furthermore, it shall establish a standardized intelligent database concerning persons who have committed tax offenses under Article 274 of the Direct Taxation Act and tax debtors, in accordance with criteria prescribed by the Council, and shall provide online access to this list for supervisory authorities, special law-enforcement officers under the Act, and the credit-rating company referred to in Articles 5 and 8 of the 2007 Act on

Facilitating the Granting of Bank Facilities, Reducing Project Costs, Accelerating Implementation of Production Projects, and Increasing Banks' Financial Resources and Efficiency. The Organization shall make issuance of tax-clearance certificates for any real estate conditional upon registration of the relevant transaction in the system referred to in Article 23 of this Regulation (Article 27 and its Notes). The Central Bank shall establish, in cooperation with covered persons and in accordance with requests from the Center, a system for identifying relationships among persons and shall enable the Center and other supervisory bodies to conduct inquiries through that system. Identification of relationships among persons means identifying persons who have relationships with one another involving guarantees, including facilities and obligations; partnerships, including joint business activities and joint accounts; credit facilities and obligations, including guarantors; powers of attorney; kinship by marriage or blood; or other relationships declared by the customer (Article 29 of the Regulation). The Iranian Association of Certified Public Accountants shall provide covered persons with unrestricted online access to audited financial statements and their appendices, audit reports, statutory-inspector reports, and other reports attached to financial statements (Article 30 of the Regulation). The Judiciary, in cooperation with the Center, shall establish the necessary electronic procedures and mechanisms for online exchange of judicial information concerning persons suspected of money laundering or terrorist financing in such a manner that the Center may submit requests electronically to the competent judicial authority for necessary judicial orders, including freezing or unfreezing assets, that information can be communicated to judicial law-enforcement officers, and that judicial decisions, including judgments and orders, can be communicated electronically to the Center and the relevant covered persons (Article 31 of the Regulation).

Electronic Funds Transfers and Correspondent Banking

Chapter Six of the Executive Regulation addresses correspondent banking and electronic funds transfers.

Cross-Border Correspondent Banking

Financial and credit institutions shall conduct an appropriate assessment of money-laundering and terrorist-financing risks in cross-border correspondent banking relationships and other similar relationships. Correspondent banks shall collect sufficient information concerning respondent banks before establishing a business relationship and continuously thereafter in order to understand the nature of the respondent bank's activities and appropriately assess money-laundering and terrorist-financing risks on an ongoing basis. Financial and credit institutions shall consider, at a minimum, the following matters concerning a respondent bank: (1) the country or jurisdiction in which the respondent bank is located; (2) collection of sufficient information about the respondent bank seeking correspondent services in order to fully understand the nature of its business and target market and to assess the bank's reputation on the basis of publicly available information; (3) the quality of supervision over the bank, including determining whether investigations or other supervisory measures relating to money laundering and terrorist financing have been or are being undertaken in respect of the bank; (4) the financial group to which the respondent bank belongs and the countries and jurisdictions in which the group's branches and subsidiaries are located; (5) information concerning the management and ownership of the respondent bank, particularly the existence of beneficial owners or politically exposed persons; (6) the purpose of the services provided to the respondent bank; (7) the nature and quality of banking regulations and supervision in the respondent bank's country, particularly anti-money laundering and counter-terrorist financing laws; (8) the respondent bank's procedures and policies for

preventing and detecting money laundering and terrorist financing, including its customer due-diligence measures; (9) the possibility of verifying the identity of third parties authorized to use the services of the financial and credit institution acting as correspondent bank; and (10) an assessment of the controls implemented by the respondent bank to combat money laundering and terrorist financing (Article 92 of the Regulation). In this regard, covered persons shall refrain from establishing correspondent relationships with shell banks (Article 93 of the Regulation).

Cross-Border Electronic Foreign-Currency Transfers

Financial and credit institutions are required to conduct all cross-border foreign-currency transfers through an approved messaging system and channels supervised by the Central Bank and, when sending such transfers, to obtain the following information: (1) information concerning the originator, including first name and surname, national identification number/national identification code/special identification number for foreign nationals, SHAHAB identification number, date and place of birth, address, and the account number through which the transaction is conducted; and (2) information concerning the recipient or beneficiary, including first name and surname/company name, bank name, and account number of the destination account (Article 95 of the Regulation).

Domestic Electronic Funds Transfers

Financial and credit institutions are required to conduct all domestic interbank electronic transfers solely through the Central Bank's national payment infrastructures, such as SATNA, PAYA, and SHETAB, and, when making such transfers, to record the following information in the relevant systems of the Central Bank of Iran: (1) information concerning the originator, including first name and surname, national identification number/national identification code/special identification number for foreign nationals, SHAHAB identification number, address, and account number/IBAN of the account through which the transaction is conducted; and (2) information concerning the recipient or beneficiary, including first name and surname and account number/IBAN of the destination account. Financial and credit institutions shall also record the following information in their own relevant systems for all intra-bank electronic transfers: (1) information concerning the originator, including first name and surname, national identification number/national identification code/special identification number for foreign nationals, SHAHAB identification number, date and place of birth, address, and the account number through which the transaction is conducted; and (2) information concerning the recipient or beneficiary, including first name and surname, national identification number/national identification code/special identification number for foreign nationals, SHAHAB identification number, date and place of birth, address, and the destination account number (Articles 96 and 97 of the Regulation). Financial and credit institutions shall refrain from issuing gift cards, anonymous purchase cards, and similar payment cards to customers who do not hold an account with the institution and shall identify within their systems the link between such payment cards and the customer's account. Such cards are subject to the rules governing cash (Article 101 of the Regulation).

Carriers of Cash, Bearer Negotiable Instruments, and Bearer Securities

Chapter Eight of the Anti-Money Laundering Regulation addresses persons who physically carry cash, bearer banking instruments, and bearer securities. Entry of bearer banking instruments and bearer securities through points of entry is permitted only within the framework of the Executive Directive on Rules Governing Foreign Currency/Banking Instruments and Bearer Securities Accompanying Travelers, issued by the Central Bank. The

Islamic Republic of Iran Customs Administration shall, in cooperation with the Center, Bank Melli Iran, and the Law Enforcement Force, establish the necessary electronic mechanism for implementation of that Directive. Where there is suspicion of money laundering, terrorist financing, predicate offenses, or the truthfulness of a traveler's declaration, Customs shall, within the framework of the Directive, retain the funds, banking instruments, and bearer securities with Bank Melli Iran and promptly report the matter to the Center for further action. Where the Center does not confirm the source of the funds or documents, it shall submit a report to the judicial authority and notify Customs not to return the relevant funds or instruments to the traveler until a final determination is made. Where the source of such funds or instruments is confirmed, the Center shall promptly notify the Islamic Republic of Iran Customs Administration that their return is unobjectionable (Article 113 of the Regulation). Persons providing foreign-exchange services and selling foreign currency are required to obtain from the applicant information concerning the purpose of receiving the service, including the destination and manner in which the requested cash funds will be spent, obtain the relevant supporting documentation from the customer, and enter the information into the relevant systems. Operating banks shall issue a banking declaration evidencing the sale of foreign currency in banknote form for purposes of taking the currency abroad by a traveler, for submission to the Islamic Republic of Iran Customs Administration. In order to reduce the risks associated with cash transfers of foreign currency, the Central Bank shall adopt the necessary measures to reduce demand for foreign-currency cash and provide non-cash alternatives to travelers leaving the country (Article 114 of the Regulation). Exit of cash, bearer banking instruments, and bearer securities through points of departure is permitted only within the framework of the rules referred to in Article 113 (Article 115 of the Regulation).

Guidelines and Training

It should be recognized that all strategies, directives, and executive policies implemented in the country, governmental institutions, organizations, ministries, banks, and covered persons ultimately depend on human resources and the diligence with which those individuals implement them. If the personnel employed have not received adequate training or do not fully understand the offense and its various dimensions, serious and potentially irreparable consequences may result. The Executive Regulation of the Anti-Money Laundering Act recognizes the importance of this matter and, in Chapter Twelve, establishes a section entitled "Guidelines and Training." Supervisory authorities are required, in coordination with and subject to the approval of the Center, to prepare and communicate to the covered persons under their supervision the feedback, guidelines, and requirements necessary for proper implementation of anti-money laundering and counter-terrorist financing regulations. Covered persons shall, in coordination with the Center, continuously assess training needs and design, implement, and evaluate programs for training and empowering their employees to combat money laundering and terrorist financing. The Judiciary, while observing Article 30 of the Code of Criminal Procedure and its Notes, shall, in cooperation with the Center, provide continuous training to judicial authorities, officials, employees, and judicial law-enforcement officers concerning the offenses of money laundering and terrorist financing and their legal dimensions as independent criminal offenses (Articles 144–146 of the Regulation).

New Technologies

Information technology, automation, modernization, and the use of modern communication tools are important elements that enhance transparency of information and, consequently, contribute to reducing money laundering

and to combating it effectively and efficiently. The Executive Regulation of the Anti-Money Laundering Act recognizes the importance of this issue and, in Chapter Thirteen, establishes a section entitled “New Technologies.” Article 147 of the Executive Regulation provides: “Financial and credit institutions and non-financial businesses and professions shall, before offering any new or special product, service, or delivery method or channel, assess the relevant risks and ensure that the mechanism for providing such products or services complies with anti-money laundering and counter-terrorist financing regulations and shall submit a report thereof to the relevant supervisory authority. Note: Supervisory authorities shall, independently of the assessments conducted by covered persons under their supervision, identify and assess money-laundering and terrorist-financing risks associated with the offering of new products, services, and delivery methods or channels within their areas of supervision. For this purpose, supervisory authorities shall, in addition to examining the use of new or developing technologies in relation to new and existing products, consider matters such as new business practices and new mechanisms for transferring and delivering goods. Ultimately, these authorities shall adopt appropriate measures for managing and mitigating such risks and shall communicate them to relevant covered persons for implementation.”

Non-Profit Organizations and Charities

In order to prevent abuse of non-profit organizations and charities, or the use of charitable and non-profit entities for money-laundering and terrorist-financing purposes, the Ministry of Interior is required to adopt appropriate measures in this regard. It shall also prevent terrorist individuals and groups from exploiting legitimate institutions in order to evade measures aimed at freezing assets (Article 148 of the Regulation).

Conclusion

Iran has acceded to several conventions concerning the combating of money laundering and corruption and has also adopted a number of significant and effective measures in this regard, including the adoption of the 2019 Anti-Money Laundering Executive Regulation. These measures are substantially aligned with the recommendations of the Financial Action Task Force, particularly with respect to accurate and comprehensive customer identification; establishment of the Financial Intelligence Center referred to in Article 7 of the Anti-Money Laundering Act; establishment of an anti-money laundering unit within each relevant body; imposition of obligations on covered persons to combat money laundering effectively; and particular attention to designated non-financial businesses and professions and the obligations imposed on covered persons and owners of non-financial businesses in the field of anti-money laundering. Other executive measures adopted by Iran to combat money laundering include retention of identity and transactional records, mandatory reporting by covered persons, establishment of effective communication and cooperation among governmental bodies, executive agencies, ministries, and organizations, training of persons who directly and practically encounter the problem of money laundering, and utilization of new technologies. Nevertheless, although the existence of laws and regulations for combating money laundering constitutes a substantial component of the deterrence mechanism and depends upon the availability of the necessary legal infrastructure, it does not in itself guarantee the absence of corruption in the country. Overall, Iran remains exposed to a high risk of money laundering, which makes combating this phenomenon more difficult. Until the country's internal structures are reformed in practical and tangible terms, anti-money laundering measures cannot achieve a high degree of effectiveness in practice. Furthermore, adequate legal supervision is not exercised over the process through which income is acquired. Despite the progress made and the measures adopted, Iran's

executive criminal policy for combating money laundering still lacks, to some extent, the necessary dynamism and operational effectiveness. Moreover, the absence of systematic coordination among governmental organizations and institutions, the lack of an efficient systematic relationship between the public and private sectors, the incomplete development of electronic government, the continued bureaucratic and paper-based operation of a substantial part of Iran's administrative apparatus and economy, and, particularly, insufficient public awareness concerning the offense of money laundering and the possibility that purchased goods or products may constitute proceeds of predicate offenses demonstrate that Iran's executive criminal policy has not yet achieved sufficient effectiveness and efficiency in the effective combating of money laundering.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Abbasi A. Combating Money Laundering in International Instruments and the Iranian Legal System. 1st ed. Tehran: Mizan Legal Foundation; 2014.
2. Miralaei N. Electronic Money Laundering from the Perspective of International Law: Majd Publishing; 2014.