



Recommendation No. 3/2008 (of November 20)
of the Board of the Hungarian Financial Supervisory Authority
On the Prevention and Combating of Money Laundering and Terrorist Financing

I. Purpose and Scope of this Recommendation

The HFSA issues this recommendation in order to ensure the uniform implementation of the obligations arising from the changes in domestic and international legal statutes accepted and published during the past years for the prevention and deterrence of money laundering and terrorist financing.

1. This recommendation is addressed to service providers supervised by the HFSA and governed by the Act on the Prevention and Deterrence of Money Laundering and Terrorist Financing.
2. This recommendation takes account of the 40+9 Recommendations of the FATF, of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter referred to as the Directive), of the special rules set forth for financial service providers in Regulation No 1781/2006/EC on information on the payer accompanying transfers of funds, of the provisions of Act CXXXVI of 2007 on the prevention of money laundering and terrorist financing (hereinafter referred to as the Money Laundering Act: MLA), of the decrees issued for its implementation, and of Act CLXXX of 2007 on the implementation of financial restrictive measures and the freezing of assets as ordered by the European Union and on the related amendment of certain Acts, and of the provisions of the model rules provided by the HFSA to the service providers.
3. With this Recommendation the HFSA intends to promote efficient practices in compliance with the law and with the Recommendations of the FATF, and to provide assistance to market participants in the development of their procedures to properly serve the prevention and deterrence of money laundering and terrorist financing.
4. The HFSA shall examine compliance with this Recommendation in the course of its procedures and shall pay special attention to the internal regulations and practices of supervised institutions for the prevention and deterrence of money laundering and terrorist financing.
5. The expectations of the HFSA are set forth in this Recommendation and in the Guidelines attached. The statutory provisions, the model rules issued by the HFSA and the other recommendations are not repeated here, i.e., if some legal statutes prescribe requirements in addition to this Recommendation, the HFSA shall also require compliance with those.

II. Customer Due Diligence Procedure

6. In order to enable the use of the concepts of business relationship and transaction order in line with the practice the HFSA deems it necessary for service providers to

differentiate between their customers in terms of whether their relationship with the customer is long-term or ad-hoc.

7. The HFSA expects service providers to interpret the concepts of business relationship and transaction order as follows, and shall proceed accordingly in the course of its examinations:

Business Relationship:

A long-term business relationship established between the customer and the service provider.

Transaction Order:

A transaction order is an occasional contact created between the customer and the service provider, in which the occasional customer “walking in” does not establish a long-term relationship with the service provider.

8. There is no need to conduct a new customer due diligence procedure in connection with every transaction order transacted (hereinafter referred to as the Transaction) within a business relationship, provided that all data required for customer due diligence are fully available to the service provider as mentioned in Section 21.
9. In order to enforce the principle of the risk-based approach, service providers shall employ all of the procedures for customer identification, but shall specify the extent of the measures to be applied by them in any given situation with consideration to the risks determined with consideration to the nature of the involved customer, business relationship or transaction.
10. The provisions of the Act with regard to customer due diligence differentiate between normal, simplified and enhanced due diligence procedures. The HFSA expects service providers to generally apply “know your customer” and “prudence in customer management” principles in the course of all of their procedures.
11. Pursuant to the best practices that have evolved in the financial markets, service providers shall prepare manuals and tables for their staff, to summarise which cases fall under which types of due diligence and with what sets of data.
12. The internal regulations should specify the business relationships, transactions, transaction orders, products and cases that represent enhanced risks and may be suitable for money laundering and terrorist financing, and which therefore require special consideration, while the same should also specify cases and products of low risk.
13. Low-risk business relationships, transactions and transaction orders may include contracts for bank cards with related accounts that enable deposits of only HUF 50,000-100,000 and where the card allows only low amounts to be withdrawn from ATMs and no other operations to be performed, or contracts for accounts that can be used only to fulfil public utility payment obligations. For such cases service providers shall record the minimum set of data for the identification of the customer, for the identification of the beneficial owner and for the business relationship and for the transaction order.

14. High-risk business relationships may for instance include transaction orders with high amounts in relation to the daily practice of the service provider, most credit relationships, unit-linked insurance contracts with high amounts in the case of insurance products, or portfolio management agreements in the case of investment services. For such cases service providers shall record the maximum set of data for the identification of the customer, for the identification of the beneficial owner and for the business relationship and for the transaction order.
15. Service providers should set forth within their internal regulations their procedures to be followed in the course of due diligence with detailed coverage on how the process and the verification of customer data, and the submitted documents, on the steps for assessing the business practices of the customer, and should summarise the typical transactions included within the service provider's scope of operations that represent enhanced risks of money laundering and terrorist financing. Training for staff should include training on the established procedures.
16. The identification of the customer shall be considered proficient and complete if performed on the basis of an authentic, authority-issued document suitable for personal identification, by a person who has been trained to conduct the identification procedure. The authenticity of the submitted documents may be established using special-purpose devices (such as UV light, a magnifier, a document data warehouse, etc.). It is desirable to record customer identification data in a retrievable way and also to periodically re-check the data.
17. If there could be doubts as to the authenticity of the documents, this is to be recorded on the customer file card and the customer identification procedure is to be performed repeatedly before the execution of any further transactions (such as the receipt or the transfer of a large amount or before an application for several cards or for a significant upward change in the card limit, etc.), or the business relationship is to be terminated.
18. Service providers shall verify the authenticity of the documents submitted in the course of due diligence measures, as well as the veracity and realistic nature of the information presented by customers. In the course of this verification service providers should use records available for this purpose pursuant to legal statutes or they should use records accessible to the public.
19. As part of their customer due diligence procedures, service providers should continuously monitor the business practices and the contacts of their customers.
20. The HFSA draws the attention of service providers to their obligation to refuse to establish or to maintain a business relationship or to carry out a transaction if they are unable to fully apply customer due diligence procedure for the affected customer.
21. As of January 1, 2009 service providers may not accept transaction orders from their existing customers who did not show up personally or by way of a proxy at the service provider for the purpose of customer due diligence measures and where the due diligence information pursuant to the MLA, in effect since December 15, 2007, and the declarations with regard to the beneficial owner are not fully available. This prohibition shall not apply to the amortisation of loans and to collections and direct debit.

Following July 1, 2009, the HFSA shall enhance its control of the implementation of this statutory obligation.

22. The HFSA deems it necessary for service providers to highlight to their customers via notifications or information bulletins that following the deadline specified in the law they shall not be allowed to execute transaction orders initiated by existing customers as long as those customers have not fully complied with their due diligence obligations.

III. Customer Profile

23. Service providers shall generate customer profiles on the basis of their customer due diligence measures and having gotten to know their customers with due care, based on a systematic analysis of their customers' financial and payment practices and on the basis of appropriate record-keeping of their customers' contacts and cash flows. The profiles thus generated should ensure the transparency and the lucidity of their customers' transactions and contacts at all times. Service providers shall examine whether or not issued transaction orders are consistent with the information and knowledge available on their customers and on their business and risk characteristics, including their sources of funds if necessary.
24. Service providers shall pay special attention to all complex and unusually large transactions and all transactions presenting unusual signals that can't be justified with easily transparent economic or legal purposes. The motives in the background of such transactions are worth examining as thoroughly as possible and the outcomes are to be recorded in writing and are to be made available to the competent authorities and auditors upon reporting or upon a request by some authority. The annex to the model rules issued by the HFSA provides guidance on the types of unusual transactions.
25. The HFSA expects service providers to operate monitoring systems to screen out transactions that prove to be unusual on the basis of the customer profiles.

IV. Declaration on the Beneficial Owner

26. In the course of customer due diligence service providers shall obtain written declarations from their customers on whether a specific transaction is executed in the customer's own name or in the name of someone else, because the service provider must be clear about the final owner of the transaction initiated by a customer who is a natural or a legal person, about the identity of the person interested in the operation being executed on the basis of an order and about the person actually issuing the order.
27. If a transaction order or a business relationship is established by a legal person, the beneficial owner shall mean the natural person holding at least twenty-five percent of the voting rights or of the property shares, as well as the natural person who is a member or a shareholder of the legal person and is entitled to elect or to remove the chief executive of the legal person or the majority of the members of its supervisory board, or the natural person who has sole disposal powers over more than fifty percent of the votes (an influencing stake) on the basis of agreements made with other members or shareholders of the legal person. For a foundation the beneficial owner shall mean the natural person who is the beneficiary of at least twenty five percent of the foundation's assets. It shall

also mean the natural person on whose order a certain transaction order is being executed.

28. If the written declaration made by the customer for the service provider states that the customer proceeds in the name and on behalf of a beneficial owner, then the declaration must contain the details of the beneficial owner as specified in the law. If there are doubts as to the authenticity of the declaration on the beneficial owner, it is to be verified using records available for this purpose pursuant to legal statutes or using records accessible to the public.
29. A beneficial owner who is not a customer of the service provider shall be named by the proxy proceeding on his/her behalf or by the customer, using data suitable for the identification of the beneficial owner, and shall support these with the available documents.

V. Simplified Customer Due Diligence

30. Service providers shall in all cases verify the required form of the due diligence obligation applicable to the specific customer. If the details of the customer on its face would result in simplified due diligence, but the service provider has doubts as to the justification for the procedure on the basis of the data, then the service provider should carry out normal or enhanced due diligence measures.

VI. Enhanced Customer Due Diligence

31. Enhanced customer due diligence measures are mandatory for customers and transactions representing a high risk of money laundering or terrorist financing. In such cases service providers shall record the maximum set of data as specified in the law. Enhanced due diligence measures are to be applied in the following cases:
 - If the customer has failed to did not show up personally at the service provider for the purpose of identification;
 - Upon the establishment of a cross-border correspondent banking relationship with a service provider domiciled in a third country;
 - Upon the establishment of business relationships with or the execution of transaction orders for politically exposed persons residing in another member state or in a third country;
 - currency exchange.
32. The HFSA expects service providers to apply enhanced due diligence measures for products, services and transactions representing a high risk of money laundering or/and terrorist financing. These could include large loans, changing the currencies of exotic countries, or unit-linked insurance contracts with high amounts.

Politically Exposed Person-PEP

33. Politically exposed persons are natural persons who are residents of a foreign country and are or have been entrusted with a prominent public function, and their immediate family members or persons known to be close associates of such persons. Only foreign

persons, i.e., persons who are residents of another member state or a third country and who qualify as such under the laws of their own countries shall be considered as politically exposed. There is no need to employ enhanced due diligence measures on domestic politically exposed persons, these customers may be subjected to due diligence measures pursuant to the general rules.

34. Service providers shall in all cases obtain written declarations from their customers who are foreign residents, as to whether or not they qualify as politically exposed persons under the laws of their countries of residence, and in what capacity if yes. If there are doubts as to the authenticity of a declaration, the service provider shall verify it through a correspondent banking relationship or using records available for this purpose pursuant to legal statutes or using records accessible to the public.
35. The HFSA expects service providers to obtain declarations from their customers holding dual citizenships as to whether or not they qualify as politically exposed persons, with the exception of foreign individuals with a permanent residence in Hungary and those who reside and conduct their life in Hungary for a period longer than 6 months and the members of diplomatic representations accredited to Hungary and their family members and staff.
36. Service providers shall develop internal policies and procedures for due diligence on politically exposed persons and shall separately monitor the accounts and transactions of such customers, and shall operate procedures – as allowed under legal statutes – that enable the service provider to identify politically exposed persons.

Correspondent banking Services

37. Service providers shall pay special attention within the framework of correspondent banking services to accept orders only from service providers that apply due diligence procedures that are consistent with the Recommendations of the FATF.
38. Prior to the establishment of a correspondent banking relationship service providers shall assess the anti money laundering and anti terrorist financing control mechanisms of the corresponding institution and shall prepare an in-depth analysis of those.
39. Service providers shall verify whether or not corresponding institutions have fulfilled their customer due diligence obligations in compliance with the 40+9 Recommendations of the FATF.
40. Special attention must be paid to banking relationships maintained with correspondent banks if they are located in countries or territories with low quality rules for “know your customer” procedures or if the country or territory qualifies as a “non cooperating country” in the fight against money laundering or terrorist financing.

VII. Information on the Payer Accompanying Transfers of Funds

41. Using FATF Special Recommendation No. VII as the basis, the European Union has issued its Regulation No. 1781/2006/EC on information on the payer accompanying transfers of funds, which is directly effective in its member states. Pursuant to this,

payment service providers shall record and forward information on the payer when transferring funds.

42. If requested by the HFSA, service providers shall provide information on funds transfers received with incomplete or missing information on the payer and on service providers that have initiated those. If a correspondent bank regularly transfers funds with incomplete information and if it fails to provide the missing information despite having been requested to do so, then the service provider shall report the most important data related to the procedures of this bank and the characteristic of the incomplete transfers, the details of the bank and the available data suitable for identification, to the authority operating as the financial intelligence unit and shall also inform the HFSA.

VIII. Customer Due Diligence Procedures performed by Other Service Providers

43. Within their internal regulations service providers should specify that they may accept the outcomes of customer due diligence measures performed by other service providers. If they accept such, then they should obtain the identification details as well as copies of other essential documents related to the due diligence measures. If the third party, despite having been asked to do so, fails to provide the requested data, then the service provider should perform the due diligence measures. The service provider should also perform the due diligence measures if pursuant to its internal regulations it may not accept the outcomes of customer due diligence measures performed by other service providers.
44. The HFSA expects the designated person or some other person obligated by the service provider to verify whether or not the received documents contain all of the information that is prescribed by the MLA or that is required to perform a complete due diligence, and whether or not the written consent of the customer is also available.
45. Service providers shall accept the outcomes of customer due diligence procedures conducted by other service providers only if they have verified that the sending service provider is a regulated and supervised institution and that it applies customer due diligence measures consistent with the Recommendations of the FATF.
46. Prior to accepting the outcome of any due diligence measures performed in a third country, service providers must always check the list issued by the minister responsible for the budget, of third countries employing due diligence procedures that comply with the legal statutes or that are equivalent to those. The HFSA expects service providers to monitor the notices issued by the FATF about countries employing due diligence procedures not consistent with its recommendation. Service providers may not accept the outcomes of due diligence procedures performed by institutions located in countries indicated in these notices and are obliged to carry out customer due diligence themselves.

IX. Screening System

47. The HFSA deems it necessary for service providers to operate monitoring and screening systems that enable unusual transactions to be recognised and to be analysed.

48. Special attention must be paid to sudden changes to the portfolio of the customer that can't be explained with usual economic events, and to every transaction not consistent with the customer profile. If there are no known or acceptable reasons for funds movements and transactions and if a transaction is suitable for money laundering and terrorist financing, then the service provider shall make a report to the authority functioning as the financial intelligence unit. The guidelines attached to this Recommendation contain some typical types of unusual transactions.
49. The HFSA expects internal regulations to contain rules on the enhanced control of overdrafts provided within the day and for the prohibition of no-cash transactions at the cashier and expects service providers to follow the corresponding practice. Regulations should provide for established procedures to enable overdrafts for the management of the daily liquidity position of the customer where the collateral is known to the service provider but will only become accessible following some deadline. Internal regulations should prohibit current account overdrafts with closed loan amounts where the amount is transferred around within the day between companies related by ownership or funding and maintaining accounts with the same service provider, where the overdraft can't be explained with real economic substance. For cash transactions at the cashier, if there are simultaneous cash withdrawals and deposits executed on the order of the same customer, then the cash withdrawal should be executed first. If there are insufficient funds for the transaction at the cashier, then the transaction order may not be executed. Where there are different customers and accounts involved in simultaneous cash withdrawals and deposits and where the funds for the deposits and for the cash withdrawals can be linked to each other, the cash withdrawals should be executed first. If the economic background of the transaction is not convincing or formal, it is justified to make an anti money laundering report to the authority functioning as the financial intelligence unit.

X. Issues Related to the Reporting Obligation

50. The HFSA expects service providers to report cases that allow for the determination of a suspicion of money laundering or terrorist financing, and to attach all documents in support of the reporting.
51. The designated person should pay attention to inform the person making the report about the forwarding of the report and should require of the authority functioning as the financial intelligence unit to provide factual feedback within an appropriate timeframe. The designated person should process the findings from the feedback received and the service provider should use the lessons learned and incorporate them into its regulations.

XI. Issues Related to the Designated Person, Internal Audit and Compliance Responsibilities

52. The HFSA expects the designated person to be a senior employee of the service provider with independent decision making powers, reporting directly to the most senior executive within the organisational hierarchy. The internal regulations must name the designated person and where possible, his/her deputy, and should also provide their direct contact details.
53. Prior to the forwarding of reports, the designated person should check them with regard to both form and substance.

54. The designated person or a person obligated by the service provider should analyse the screened transactions and should report without delay those, in relation to which some data, facts or circumstances emerge that indicate money laundering or terrorist financing. The designated person must participate in the creation and operation of the control mechanisms. It is the responsibility of the designated person to provide training regularly, but at least once every year, to employees, agents and contractors performing outsourced activities. The HFSA expects the service provider to verify the efficiency of the training and the knowledge of the employees by way of examinations.
55. The designated person or a person obligated by the service provider should regularly verify whether or not the agents of the service provider or its contractors performing outsourced activities perform their anti money laundering and anti terrorist financing procedures in compliance with the regulations of the service provider.
56. The compliance organisation of the service provider should verify the adequacy of the processes to be completed in the course of its anti money laundering and anti terrorist financing activities. If the financial organisation does not operate a compliance function, then the mentioned responsibilities should be performed by the internal audit function.

XII. Issues Related to Financial Restrictive Measures and the Freezing of Assets ordered by the European Union

57. The HFSA expects service providers to use and where necessary to update the documents published by the European Union that contain the lists specified by the annexes of the council regulations (council regulations 881/2002/EC and 2580/2001/EC) created to combat terrorist financing and to be applied directly. These provide the lists of the natural and legal persons and groups that are subject to international sanctions. Transactions are to be examined with regard to whether or not they may be connected to specific persons included on the mentioned lists. Service providers should confirm whether or not the details of persons included on the list match the details of their customers. Where there is indeed a match of details, the designated person should make a report to the authority operating as the financial intelligence unit.
58. The service provider should also be familiar with other lists available on organisations and individuals connected to terrorism, such as the international lists officially published in Hungary by the authorities of the USA, the UNO and of other countries, and in the case of groups of companies the records made available by the foreign owner.
59. Special attention must be paid to non customary amounts sent and received electronically, in specific with regard to the size of the amount, to the beneficiary destination country and to the country of the payer, as well as to sudden changes in currency, to the use of new currencies, and to the exchange of assets in complicated transactions without a justification with regard to economy or efficiency.
60. The financial conduct and practices of non-profit and charitable organisations are to be examined and assessed. Financial service providers must take special care in the analysis if the conduct is not consistent with the reported and registered scope of activities of the

organisation or if the origins of the funds received are not clarified, or if sums accumulate from other than the customary sources, or if the previous activities of the organisation do not justify their intended use or if the destination country or the payee raises suspicion.

Closing Provisions

This Recommendation is a legal instrument pursuant to Section d) of Paragraph (1) of Article 12 of Act CXXXV of 2007 on the supervision of financial organisations by the state, the provisions of which also extend to service providers that are new entrants to the market in addition to those that are already in operation.

The substance of this Recommendation issued by the Board of the HFSA expresses the requirements set forth in legal statutes, the principles and methods recommended for application on the basis of the law enforcement practice of the HFSA, as well as market standards and usual practices. The HFSA shall audit whether or not the provisions of the regulations of financial organisations comply with this Recommendation issued by the Supervisory Council and shall compare these to the related practices of the service providers. Upon non compliance in practices the HFSA shall call upon the service provider to develop regulations that are consistent with this Recommendation.

This Recommendation replaces Recommendation No. 1/2004 on the prevention and deterrence of money laundering.