Due Diligence Procedures For Customers of Prepaid Cards

In the Arab Republic of Egypt

March 2019

Due Diligence Procedures
For Customers of Prepaid Cards

In the Arab Republic of Egypt

جمهورية مصر العربية

وحدة مكافحة غسل الأموال وتمويل الإرهاب

Table of Contents

Introduction

Law No. 80 of 2002 Promulgating the Law on Anti-Money Laundering identified, in Article 1-C thereof, the financial institutions governed by the Law, on top of which are public banks in Egypt, their branches abroad and branches of foreign banks in Egypt. In Articles 8 and 9, the Law stipulates certain conditions, the first is the enforcement of customers due diligence procedures, in addition to other regulations and measures relating to combating money laundering and combating terrorism that are issued by EMLCU. The Executive Regulations of the Law issued by the Prime Minister by virtue of Decree No. 951 of 2003 and its amendments, explain in Article 3 thereof, EMLCU's mandates, including laying these regulations and procedures, and verifying, in coordination with supervisory authorities, abidance of financial institutions by these rules.

These Procedures have been laid in line with EMLCU's determination to cope with developments taking place worldwide standards, especially concerning financial inclusion requirements, as EMLCU strives to ensure that no obstructions impede realizing the objectives intended by the requirements of combating money laundering and financing terrorism. Prepaid card services are one of the financial services that are capable of achieving financial inclusion owing to the simple procedures required for issuing them and since they provide multiple services, such as cash deposit and drawing, as well as payment for purchases.

As CBE and banks set ceilings for transactions taking place using prepaid cards, thereby lessening their associated risks, and since monitory frameworks obligate banks to set effective monitory systems and measures for monitoring transactions taking place through these services, hence, these procedures have been prepared in light of the risk-based methodology adopted by the Financial Action Task Force (FATF), which allows for the application of simplified procedures over risks concerning money laundering and financing terrorism.

In enforcing of the law on Anti-Money Laundering & its Executive Regulations referred to hereinabove, all banks operating in Egypt, all their branches and affiliates located in Egypt and abroad, and all branches of foreign banks operating in Egypt, shall abide by these procedures, shall take them into account and shall implement them accurately when providing prepaid card services in order to realize the aspired objectives of combating money laundering and financing terrorism. An exception to the foregoing are prepaid card services for which exceptional approvals are issued by Head of the Board of Trustees of EMLCU in support of national initiatives, as it is essential to abide by the contents of such approvals on customers due diligence procedures.

According to CBE's definition on the issuance date of these Procedures, micro enterprises and companies shall mean those whose annual return (annual sales and revenues) are less than one million Egyptian Pounds, or with a paid in capital of less than EGP 50,000 for enterprises and companies, which have been exercising their activities for less than a year.

Definitions

The following words and expressions shall have the meanings set for the below where is they appear in these procedures

The Service(s)	Payment services using prepaid cards provided by public banks in Egypt and its branches abroad.
Actual Beneficiary	A natural person unto whom the title or control of the customer shall actually devolve, or a person on behalf of which an operation is carried out, including persons who have actual control over a customer, whether the latter is an in kind person or a legal arrangement.
The Unit or EMLCU	The Egyptian Money Laundering Combating Unit
Service Provider	The entities which the bank enters into contract for the provision of prepaid card services, according to the regulations issued by CBE in this regard.
Customers Due Diligence Procedures	Customer identification rules issued by EMLCU in 2011 and all amendments thereto issued by EMLCU.
Micro Companies and enterprise	Enterprises and companies defined as such, according to the definition issued by CBE.*
Blacklists	Includes lists of terroristic entities and terrorists, regulated by Law No. 8 of 2015, statements issued by the UN Security Council concerning financing terrorism and financing the proliferation of weapons of mass destruction, and any other lists which the bank may prepare or may regard as necessary to refer to.
Freezing of Funds	Temporary prohibition of transferring, moving, replacing, wiring or disposing of funds.
Competent Officer	The officer in charge of applying customer identification and verification procedures in the cases provided for in these procedures, whether such officer works at a bank or a service provider.

*According to CBE's definition on the issuance date of these Procedures, micro enterprises and companies shall mean those whose annual return (annual sales and revenues) are less than one million Egyptian Pounds, or with a paid in capital of less than EGP 50,000 for enterprises and companies which have been exercising their activities for less than a year.

2- Scope of Validity of Procedures

2-1 The rules regulating the issuance of prepaid cards and the Anti-Money Laundering (AML) Regulations for Banks issued by CBE, and any amendments thereto, shall apply over prepaid card customers. Any other matters not provided for in these Procedures concerning prepaid card customers, shall be regulated by the Bank Customers Due Diligence Procedures, according to the nature of the service.

2-2 These regulations shall only apply over customers and real beneficiaries, including natural persons and micro- enterprises and companies, while Bank Customers Due Diligence Procedures shall apply over customers other than the foregoing. An exception to the foregoing shall be the rules on transfers mentioned in clause 9 of these Procedures, which shall apply over all types of customers.

2-3 In case the identity of a customer who is an Egyptian natural person has been identified according to the Bank Customers Due Diligence Procedures using another document
other than a national ID card, in this case, the bank must examine the customer's original ID card and take a photocopy of it, which shall be signed by the competent officer, establishing it is an exact copy. It must be verified that the ID card is valid and that its data has not been tampered with.

2-4 These Procedures shall not apply over customers of any other products or services provided by the bank, except as approved by the President of the Board of Trustees of EMLCU. He may also approve exceptional due diligence procedures that differ from these Procedures, for prepaid cards services that support national initiatives.

3- Use of Service Providers for Customer Identification and Verification

3-1 A bank may engage a service provider to apply customer identification and verification procedures mentioned in clause 5 of these Procedures, in the following cases:

3-1-1 If the service provider is a mobile network operator authorized by the competent authority to operate in Egypt in accordance with Law No. 10 of 2003, whether the service was provided through one of its fixed or moveable branches or outlets, provided that the customer identification and verification procedures shall be carried out by one of the aforementioned company's employees.

3-1-2 If the service provider is one of the offices of Egypt national postal authotity (Egypt Post), provided that the customer identification and verification procedures shall be carried out by one of Egypt Post's employees.

3-1-3 If the service provider is a civil society association or organization licensed by FRA to carry out micro finance activities in accordance with the provisions of Law No. 141 of 2014 and the decrees issued in execution thereof, provided that the following conditions are met:

3-1-3-1 The entity must have a valid commercial register and a valid tax card if it is a company, or statutes ratified by the Ministry of Social Solidarity if it is a civil society association or organization.

3-1-3-2 A letter shall be obtained from FRA establishing its approval that the entity become a service provider.

3-1-3-3 The service provided by the entity shall be restricted to its customers obtaining micro finance only, in compliance with the provisions of Law No. 141 of 2014 and the decrees issued in execution thereof.

3-1-4 If the service provider is a governmental entity or a public sector unit, via one of its competent departments, after obtaining a written approval to this end from CBE.

3-1-5 If the service provider is another entity other than those mentioned in the previous clauses, provided that the following conditions are met:

3-1-5-1 The entity must have a valid commercial register and a valid tax card.

3-1-5-2 If the entity provides a service through one of its outlets located at another entity, the other entity must have a valid commercial register and a valid tax card.

3-1-5-3 The bank shall render the entity owners and managers subject to the Bank Customers Due Diligence Procedures and shall collect any information it deems necessary about them.

3-1-5-4 The bank shall verify that none of the entity owners and managers are subject to any
penalties for any crimes or any dishonouring conduct.

3-1-5-5 The terms & conditions contained in the contract concluded with that entity shall stipulate setting up systems and measures that would ensure that this entity's employees and its outlets' employees as well, enjoy high standards of competency and integrity. Such procedures and measures shall at least ensure inquiring about the employee's former career/ posts and obtaining criminal clearance statements.

3-2 In all the previous cases, the following regulations shall apply:

3-2-1 The bank shall set customer identification and verification measures in line with the provisions of clause 5 of these Procedures. The service provider shall apply these procedures in its capacity as the bank's agent while the bank shall be fully responsible for the soundness of these procedures and their efficient implementation.

3-2-2 The bank shall lay appropriate measures to regularly verify compliance of service providers with customer identification and verification procedures. in case there are any material or repeated violations in this regard, according to the standards set by the bank, the bank shall reconsider whether it would be appropriate to continue to use the service provider's services to apply customer identification and verification measures or not.

3-2-3 The contract signed between the bank and the service provider should state the obligations and responsibilities of each party with regard to applying customer identification and verification measures, including the service provider's commitment to allow CBE's inspectors to visit the premises where the services are provided in order to verify the sound and effective enforcement of these procedures.

3-2-4 The bank shall verify that employees at the service provider's branches and outlets receive the necessary training on customer identification and verification measures.

3-2-5 The service provider shall provide the bank with all the documents relating to providing the services to customers within thirty days at the most as of the commencement of the service. In case of non-abidance by the foregoing, the service shall be terminated. During that period, the bank shall carry out the necessary measures for managing risks of money laundering and financing terrorism, including setting limits for the number, values and types of transactions that may be carried out.

4- Customer acceptance Policy

4-1 The bank shall lay clear policies and procedures for accepting customers that would help realize financial inclusion, provided that these procedures specify the circumstances under which the bank may not accept a new business relation or which may require termination of an existing work relation as a result of being exposed to unacceptable levels of risks of money laundering and financing terrorism, which includes finding out that a customer is listed on a blacklist, and the bank shall consider sending a suspicion notice to EMLCU according to stipulated reasons for terminating a work relation.

4-2 The aforementioned policies and procedures must particularly indicate the categories of customers that may expose the bank to larger risks and shall consider applying the provisions of clause 8 of these Procedures over them.

5- Customer Identification and Verification

5-1 General Provisions

5-1-1 The bank shall be responsible for the management of risks relating to money laundering and financing terrorism with regard to the provision of the service, which may include, as deemed necessary, obtaining any additional information or documents not mentioned in these Procedures or applying Bank Customer Due Diligence Procedures, according to the risks evaluated by the bank for each customer, separately.

5-1-2 The bank shall not provide this service to unknown persons or persons who apparently have fake names.

5-1-3 Customer identification and verification shall take place using original documents, or information and data taken from original sources that are both reliable and independent.

5-1-4 An exception to the application of customer identification and verification procedures, shall be granted customers whom the bank already subjected them to Bank Customer Due Diligence Procedures, unless the bank has doubts with regard to the accuracy of the data previously obtained thereby, or believes that such data is insufficient and needs to be completed.

5-1-5 The bank must verify that a person requesting to act on behalf a customer, is authorized to do so. Further, the customer identification and verification procedures shall apply over this person pursuant to clause 5-2 of these Procedures.

5-1-6 The bank shall check the real identity of the beneficiary and shall take reasonable measures to carry out this identity check using information or data provided by reliable and independent sources, to ensure the bank convincingly reveals the beneficiary's real identity. The bank may check the identity of the real beneficiary after the commencement of the work relation according to the following conditions:

5-1-6-1 That this takes place as soon as possible.

5-1-6-2 That this was necessary in order to avoid interrupting the normal course of business.

5-1-6-3 In case of the effective management of risks of money laundering and financing terrorism.

5-1-7 In cases of customers that are micro enterprises or companies, the customer ownership and control structure must be understood well, and the real beneficiaries must be identified, provided that the actual beneficiary identification and verification procedures shall include the following:

5-1-7-1 Natural persons owning a dominant share in the company or enterprise (if any).

5-1-7-2 Natural persons who do not own a dominant share in the company or enterprise but have control over them by any other means (if any).

5-1-7-3 Natural persons in charge of the actual management of the company or enterprise, in cases where the previous two conditions do not apply over these persons.

5-1-8 The bank shall verify that the application submitted for the provision of services has been completely filled out (a unified application form for the service issued by the bank) and signed by the customer or the authorized person (in cases of micro enterprises or companies) in front of the competent officer.

5-1-9 The bank must understand the objective and nature of the dealings. However, in cases where the objective and nature of the dealings are clear to the bank, the bank may insert them in the application form without asking for relevant information or documents from the customer.

5-1-10 The bank shall obtain accurate information relating to the customer's profession or industry and shall not accept any unclear statements that do not reflect a clear industry.

5-1-11 Customer identification and verification procedures may take place at the customer's premises by any of the competent officers.

5-1-12 If the bank is unable to satisfy customer identification or verification measures pursuant to these Procedures, it shall not provide the service and shall consider sending a suspicion notice to EMLCU with regard to this customer for reasons causing non-satisfaction of the Procedures.

5-1-13 The bank shall carry out its obligations mentioned in the Executive Regulations of the Law on Anti-Money Laundering concerning the execution of the resolutions adopted by the Board of Directors with regard to combating financing terrorism and the proliferation of weapons of mass destruction, besides the procedures and techniques issued by EMLCU and CBE in this regard, including checking to what extent a customer is enlisted on any blacklist prior to approving the provision of the service, while paying due regard to
checking again whenever these lists are updated and taking the necessary measures to freeze funds in accordance with the relevant laws, regulations, procedures and techniques.

5-1-14 With regard to foreign customers, the bank shall restrict the use of cards issued for them to domestic uses (inside Egypt only), except in cases for which both CBE's and EMLCU's consent has been obtained.

5-2 Customer Identification and Verification for Natural Persons

5-2-1 Obtaining the Required Information for Identification
A bank shall check a customer's identity by obtaining the following information at least prior to providing the service:

- Full name as per the identity card.
- Nationality.
- Birth place and date.
- Gender (M/F)
- Current permanent residence.
- Mobile No.
- Landline No. (if any).

- Profession or job.
- Workplace and address.
- National ID No. for Egyptians.
- Passport or travel deed No. for non-Egyptians.
- Customer's undertaking that he is the real beneficiary of the service and identifying the real beneficiary, if any.
- Customer's undertaking to update his data as soon as any changes occur thereto or as requested by the bank.

5-2-2 Verification Measures

5-2-2-1 Prior to the provision of the service, the bank shall review the customer's original personal identification deed to verify the soundness of the data and information obtained, and shall obtain a photocopy of this deed, to be signed by the customer to establish that it is an exact copy. Personal identification deeds accepted by the bank to verify a customer's national ID No. shall be restricted to the customer's national ID card, passport or travel deed. In all cases, the aforementioned instrument must be valid and shall not be accepted if there are any clear evidence of any tampering.

5-2-2-2 if the customer's identification instrument does not include his permanent residence or profession, or if any of them is different than what is written in the service application form, such information must be verified through original documents, or by information and data obtained from a reliable independent source, which may take place after beginning the provision of the service in accordance with clause 5-1-6, provided there are limits on the number, value and type of operations that can be carried out until the aforementioned documents, information or data are obtained.

5-3 Identification and verification procedures for customers, which are micro enterprises and companies

5-3-1 Obtaining the necessary information for customer identification
The bank shall obtain the following information before providing the service:

- Name (tradename).
- Legal form (as per the commercial register or the license for exercising the activity, if any).
- Nature of the activity.
- Address of the headquarters.
- Mobile phone No. of the company or enterprise's authorized signatory.
- Landline No. (if any).
- Commercial Registration No., date and place (in case of issuance of a commercial register).
- No. and date of the necessary license for exercising the activity issued by a governmental authority, if such license is issued (for entities for which a commercial register has been issued).
- Data on the activities as extracted from the documents or other trusted sources, other than the customer (for entities for which neither a commercial register or a license are issued for exercising its activities).
- Names, addresses and nationalities of those owning a share exceeding 25% of its capital. If none of the partners own this percentage, the same information shall be obtained for the partner owning the largest interest. In case all title shares are equal, this data shall be obtained for the partner, which the bank estimates, according to the standards set thereby, that he controls the company or enterprise by any other means (if any).
- Names, addresses and nationalities of the person or persons responsible for the actual management of the company or enterprise.
- The authorized person's undertaking to update the customer's data as soon as any changes take place or upon the bank's request.

5-3-2 Verification Measures

5-3-2-1 The bank shall check the company or enterprise's delegation documents, authorizing the natural person(s) to represent it.

5-3-2-2 Prior to providing the service, the bank shall obtain a valid official extract of the customer's commercial register, or the necessary license issued by a governmental authority to exercise its activities for entities for which commercial registers are not issued. Concerning entities for which neither a commercial register or a license is issued for exercising their activities, the customer's activities shall be checked using the documents, data or information obtained from other reliable sources other than the customer, besides the ID card of the enterprise or company employer/ owner, as per clause 5-3-1, and the company or enterprise's authorized signatories. The bank may also obtain additional documents from the customer (such as a tax card, contract of incorporation, or other relevant documents) according to the bank's assessment of the volume of the customer-associated risks. In all cases, such documents must be valid and none of them shall be accepted if there are any clear signs of tampering with them.

5-3-2-3 The bank shall verify the soundness of the information on the customer by checking his original documents provided by the authorized signatory and shall take a photocopy of same, while the competent officer shall sign each of them, indicating it is an exact copy.

6- Data Updating

6-1 For customers who have been subjected to customer identification and verification measures according to these Procedures, the bank shall regularly and adequately update such data, information and documents it had obtained when applying these measures. Such updates shall take place every five years at the most, which period may be shortened if the bank estimates that there are high risks associated with the customer. In low risk cases, the bank may update the data through electronic means.

6-2 For existing customers prior to the issuance of these Procedures, the bank shall subject them to the identification and verification measures as per these Procedures, based on the extent and the relative weight of the risks, while requiring the updating of the data if the bank has any doubts with regard to the accuracy of the data previously obtained from the customer upon starting the work relation with it, or if the bank estimates that such data is insufficient and needs to be completed, provided that all such customers shall be subject to these measures within three months at the most. If the identity verification measures mentioned in clause 5-2-2 were previously taken when providing these services to these customers, the bank may obtain the additional data or information that is required in accordance with clauses 5-2-1 and 5-3-1 through electronic means.

7- Constant Operation monitoring

7-1 The bank shall lay an internal system that allows for the constant monitoring of the operations, which shall include the inspection of the operations taking place throughout the relation period with the customer to ensure compliance of the operations taking place with the customer information, its activity type and its associated risks, including the source of funds, if deemed necessary.

7-2 The bank shall give special attention to all unusually complex and large operations or irregular operations, in cases where such operations or types of operations do not have clear legitimate or economic purposes. Such operations and types of operations shall include the following:

- Operations that exceed any ceilings set by the bank leading to irregular transactions.
- Complex or large operations in comparison with the customer's previous nature of activities and dealings.
- Division of transactions to be less than the ceiling set by the bank over several transactions or cards that seem to be related.

7-3 The bank shall examine the background of the transactions and the purpose thereof as far as possible and shall record the results reached in accessible records. It shall keep such results for at least five years to give competent authority access thereto when exercising its mandates.

8- Risk Management relating to Money Laundering and Financing Terrorism

8-1 Risk Assessment

The bank shall take the appropriate steps to determine, assess and understand the risks of money laundering and financing terrorism relating to the service, while taking into consideration the provisions of the clause on management of risks relating to money laundering and financing terrorism mentioned in the Bank Customers Due Diligence Procedures according to the nature of the service, as well as the Annex attached hereto "Guidance on the Management of Risks Relating to Money Laundering and Financing Terrorism regarding Prepaid Card Services", while taking the following into consideration:

- Examining all risk factors related to money laundering and financing terrorism when determining the level of risks and the type and level of procedures that must be taken to mitigate these risks.
- Documentation of risk assessment conducted by the bank.
- Updating of risk assessment on a regular basis, and whenever deemed necessary.
- Provision of appropriate mechanisms to make available the information relating to risk assessment and the results reached by each of CBE and EMLCU, including cases where there are serious obstructions affecting the bank's ability to manage risks relating to money laundering and financing terrorism with regard to the service, based on the assessment.

8-2 Risk Mitigation

The bank shall carry out the following:

- To set internal control policies and systems as well as procedures that are ratified by the Board of Directors on the management of risks relating to money laundering and financing terrorism with regard to the service set out by the bank or on the level of the state, and to mitigate same, which shall include setting daily and monthly ceilings for the numbers and values of operations taking place through the service, to monitor the implementation of these policies, systems and procedures, to revisit them on a regular basis and introduce the necessary amendments in line with risk assessment results.
- To take strict measures with regard to customers which the bank estimates to have high risks as per the Bank Customer's Due Diligence Procedures.

9-Transfer Regulations

If the bank discovers that any parties to a wire transfer is listed on any blacklist, the bank must not carry out the wire transfer and must take the necessary measures to freeze its funds in accordance with the relevant provisions of the laws, regulations, procedures and techniques. The bank shall also consider sending a suspicion notice to EMLCU based on the reasons for being listed on that list. In all cases, the following rules and procedures shall apply:

9-1 In cases of domestic transfers:

9-1-1 The bank from which the wire transfer is outgoing, shall obtain information on the transfer applicant, shall verify its accuracy, maintain such applicant and shall fully include this information in the transfer message. This information shall include the following:

9-1-1-1 Name of the applicant requesting the transfer.

9-1-1-2 Card Account No. from which the transfer is being made.

9-1-1-3 Address of the transfer applicant or his ID card No., or date and place of birth.

9-1-1-4 Account No. of the beneficiary receiving the transfer.

9-1-2 Regarding transfers of sums below EGP 10,000, the information mentioned in clause 9-1-1-3 below shall not be required to be mentioned in the transfer message.

9-1-3 In case of technical problems that prevent the bank from inserting the information mentioned in 9-1-1 in the transfer message, the bank may be exempt from inserting such information if it is able to provide it to the beneficiary bank or to the competent authority, upon request, by other means within three working days, provided that the bank, in this case, inserts the card account No. from which the transfer is made in the transfer message.

9-1-4 The bank can rely on the information previously obtained thereby using the customer identification procedures to satisfy some information requirements for completing the transfer, whenever appropriate/ applicable, without any need to repeat obtaining such information and verify same when implementing the transfer.

9-1-5 In case several wire transfers are made at one time (in one batch), upon the same customer's request, such batch of transfers, must include the information required in the wire applicant mentioned in clause 9-1-1.

9-1-6 In case the bank is unable to satisfy the conditions mentioned in clause 9-1, it must not carry out the wire transfer.

9-2 In case of receiving a domestic or international wire transfer

9-2-1 The bank shall adopt reasonable follow up measures afterwards or on the spot, if possible, to identify transfers with incomplete information in the transfer application as per clause 9-1. In cases of international wire transfers, it should be verified that the beneficiary name is inserted in addition to the information mentioned in clause 9-1.

9-2-2 The bank shall adopt risk-based policies and measures to determine when to implement, reject or suspend transfers that do not include the required information regarding each applicant and beneficiary, as well as follow up measures that must be taken in each case.

9-3 In case the bank is a Mediator in the transfer process

9-3-1 The bank shall verify the extent with which all the information mentioned in clause 9-1 is inserted, besides the beneficiary name in cases of transfers incoming from abroad.

9-3-2 In case of technical restrictions that prevent keeping information on the transfer applicant or beneficiary in the transfer message, the bank shall keep all the information received by the transferor for the period of five years at least as of the date of carrying out the wire transfer.

9-3-3 The bank shall take reasonable measures compliant with straight through processing to determine the wire transfers that do not include all required information concerning each of the transfer applicant and beneficiary.

9-3-4 The bank shall adopt risk-based policies and measures to determine when to carry out, reject or suspend transfers that do not include the required information regarding each of the applicant and the beneficiary, as well as follow up measures that must be taken in each case.

Annex- Guidance on the Management of Risks relating to Money Laundering and Financing Terrorism for Prepaid Card Services

When conducting risk assessment concerning these services, the following should be generally taken into consideration: restrictions on the volumes and sources of money added to the card and the fields in which they can be used, as well as the number of cards that can be issued to one customer, and the ability of the bank's internal control system to detect same. The number of these factors and the relevant weight of each, shall be among the most important sources for forming the complete picture of risks on money laundering and financing terrorism associated with these services.
During the assessment by the bank of risks of money laundering and financing terrorism in prepaid card services, it shall take into consideration that the following indicators may increase the risks associated with these services:

- The possible use of these cards to transfer funds and the degree of speed with which the transfer takes place.
- Cases of untraceable transfers.
- Cases where it is not possible to have a comprehensive vision of all the customer's dealings.
- When the nature of the card does not allow for direct interaction with the customer in any phase of the relation with it.
- When there is high acceptance of the card as a payment tool in different fields and locations including cross borders.
- The ability to reload the card, especially with cash.
- The ability to withdraw cash from the card.

First: Card Associated Risk Factors

It is important to consider several effective factors in the assessment of risks concerning money laundering and financing terrorism relating to prepaid card services, as outlined hereinafter:

1- Geographic Location of the Card

The ability to use the card cross borders is one of the elements that increase risks of money laundering and financing terrorism, especially if it is permissible to use the card in countries that have serious shortcomings in combating these two issues.

2- Card Use Features

Whether the card requires entering a PIN and to what extent the username and his picture is placed on the card, which could limit its fields of use, especially when it comes to transferring amounts to others.

3- Available Information on Cardholders

Available information on cardholders and other parties engaged in the service are deemed the most important factors that can enable risk management concerning money laundering and financing terrorism. The availability of abundant information and the ability to verify this information is one of the factors that help reduce risk levels. For instance, this provides great ability to check the names of cardholders on blacklists.

4- Identified Card Uses

Prepaid cards are issued for a variety of uses. As long as the domains of uses are reduced (such as being limited to a certain category of merchants or with pre-set financial ceilings with regard to the volume and number of operations), this serves as a factor for reducing risks. The more the fields of uses increase, the more the risks increase.

5- Sources of Funds

a- Sources of Money

The means used to add funds to a card is one of the factors of determining associated risks. The more the controls over the sources of funds, the less are the risks. For instance, cards managed on behalf of governmental bodies for providing services to the public and payroll cards have one main source of funding, which reduces risks associated with these cards as compared with other cards which do not have the same features in terms of sources of funding.

On the other hand, unknown sources of funds added to cards, is one of the factors that increase risks. For instance, risks are high when cash is added without adequate controls or when adding money takes place using another payment tool that allows for hiding the source or the owner of the funds, or in cases when adding money takes place through wire transfers from anonymous sources.

b- Limits on Transactions

Limits placed on card transactions are considered one of the factors of risk management. The degree and nature of limits placed on dealings are among the factors that determine the level of

associated risks. For instance, the ceiling of funds that may be deposited into a card, its maximum allowed balance, the number of times the card can be recharged, are all important determinants of the level of risks.
The higher these limits are more controlled, the lower the risks are, and the lower the limits are, the higher the risk become.

c- Cash Deposit

The ability to deposit cash to the card is a high risk factor. Risks automatically decrease when sources of card funds are non-cash, such as in the case of governmental payments.
In cases of deposit cash, so long as this takes place within set limits that are in line with the risk appetite, and so long there is information on the person adding the money (such as asking for an ID card when depositing the money into the card), this decreases the level of risks.
On the other hand, risks increase whenever the limit of cash deposit increases, especially if no information is obtained on the depositor (such as in cases where deposits take place outside of banks, such as through a merchant).

d- Loading cards through other means of payment

Cards that may be loaded by other cards bear higher risks since they do not require direct contact with bank officers.

6- WithDrawing Cash from ATMs or other means:

Cards that do not allow their holders to withdraw cash using an ATM or any other means are less risky. Whenever the option of withdrawing cash exists, the higher risks become. An exception to the foregoing is withdrawing cash for expected uses (such as governmental payments and other similar programs).
It is worth noting that one of the known trends is withdrawing cash although this unsupported by the card's features. This takes place when shopping at a merchant for amounts exceeding the value of the purchased goods and receiving the difference in the value of goods from the merchant in cash.

7- Validity Period of Cards

So long as the card has a validity period, and the shorter this period is, the lower are the related risks.

8- The number of cards issued to one customer

The ability to determine the number of cards issued for one customer is one of the most important factors determining risks. This can take place by tying the cards issued to a customer with a single identifier (such as a national ID No. for Egyptians and a travel deed for non-Egyptians). Hence, risks become higher with card programs that allow a customer to have several cards, or if this takes place as a result of insufficient information to place limits in this regard.

Second: Risk Factors relating to the Card Program

1- Parties of the Card Program

The issuance of prepaid cards usually involve several parties (issuing entity, program director, distributer, service provider…etc.). The increased number of these parties usually lead to risks of losing information or non-identification of responsibilities relating to combating money laundering and financing terrorism, a matter which requires the bank to have full understanding of all the parties of the program, to clearly identify responsibilities in writing and to be aware of the impact this has on the volume of associated risks.

2- Designing the Card Program

When developing the prepaid card service or when modifying an already existing prepaid card service, it is essential that such phase includes conducting a study of the risks of using the product in money laundering or financing terrorism. The service shall therefore not be launched without obtaining the approval of the compliance department and other competent departments concerned with risk studies at the bank. Further, in light of the identified and assessed risks, internal control systems should be laid that would mitigate risks and render them controllable by the bank.

3- Designing the Card Program

It is essential that the identification and verification procedures of customers and real beneficiaries be compatible with the volume of risks borne by the card. Since Customer Due Diligence Procedures for prepaid card customers are simple measures that suit covering low risks in light of the controls set in accordance with the rules regulating the service issued by CBE, therefore the bank should understand that, in cases of high risks, it should apply customer due diligence measures that suit the level of risks, that may be stricter than those measures herein mentioned.
Further, the bank should understand the exceptional nature of prepaid cards, meaning that a cardholder may be other than the customer requesting issuance of the card (such as in cases of gift cards). Hence, when determining risks, the volume of information available on the cardholder should be taken into consideration.

4- Transactions Monitoring

Procedures followed by the bank for monitoring transactions on the card should be compliant with the associated risks of money laundering and financing terrorism.
The monitory level should increase if the card enjoys features and authorities that increase risks. The same should apply in cases of the increase of transaction value, increase of the total amounts of transactions, increased card loading frequencies or use of card in unexpected geographic locations.
With regard to cards with one main source for adding funds, such as governmental cards, the addition of money to the cards from other sources, is one of the factors that shall require monitoring. Monitory procedures shall consider the number of cards issued to one customer.
It should be taken into consideration that risks are less when cards are directly issued by the bank than when several parties are involved in the card issuance process, which would, in turn, affect the monitoring degree of the Transactions. In addition, risks are smaller when issuing cards to existing bank customers than when issuing them to new customers.

Concerning uses of the card, the following factors shall require higher levels of monitoring:

- Unusual levels or frequency rates of using cards through ATMs.
- Increased volume or number of transactions carried out over the card.
- Unexpected use of the card in a different geographic location or in a high risk country.
- The occurrence of incidents similar to trends known to be related to money laundering and financing terrorism.

5- Records

Records shall be maintained of the transactions taking place using the prepaid cards according to the records requirements mentioned in the controls on combating money laundering and financing terrorism issued by CBE, provided that the records contain adequate data on each operation separately, including electronic data on the operations, such as IP addresses and other electronic records that demonstrate all operation details.

6- Use of Service Provider

In many cases, a service provider is the party directly dealing with the customer, which allows it the chance to detect unusual acts/ trends of customers. Hence, the bank should provide the service provider with a mechanism that would enable it to send such acts/ trends to the bank in order to take the necessary measures of inspection, investigation and report to EMLCU any suspicious transactions that may be part of acts of money laundering or financing terrorism, or any attempt to carry out such acts.

7- Awareness and Training

Those in charge of the development and management of prepaid card services, shall be provided training on the risks of money laundering and financing terrorism. Such training shall also be extended to those who may be appointed for the provision of these services, especially those authorized to carry out customer identification and verification procedures. The bank shall update and develop the information it already has on trends followed to use prepaid cards in money laundering and financing terrorism, by using all available means and tools on domestic, regional and international levels.