Payment Services Using Prepaid Cards Regulating

In the Arab Republic of Egypt

Payment Services Using Prepaid Cards Regulating

In the Arab Republic of Egypt


البنك المركزي المصري
CENTRAL BANK OF EGYPT

Table of Contents

Introduction

Within the context of achieving financial inclusion and to shift towards a cashless society, and in order for everyone to have access to banking services, including the poor, youth and residents of remote places, the objective of using prepaid cards is to provide a means of payment to all classes of the society. which would ultimately expand the base of bank customers and would help achieve financial inclusion.

Definitions

The following terms and expressions shall have the following meanings assigned thereto whenever mentioned in these regulations:

Prepaid Cards	Payments Electronic cards charged in advance by customers. They may be used in purchases, transfer & withdrawing of cash based on the card balance. Prepaid cards are divided into four different types of cards, namely open, semi-closed, semi-open and closed prepaid cards.
Open Prepaid Cards	There are no restrictions/ conditions on these cards, as they may be used for withdrawing cash, depositing, transferring or receiving transfers, as well as for purchase transactions via POS terminals or via e-commerce. They may also be used at merchants/ entities/ companies without specifying them.
Semi-Open Prepaid Cards	These are cards that can only be used for purchases using POS terminals or via e-commerce. They cannot be used to withdraw cash and it can be used at any company/ entity without being specified, such as gift cards.
Semi-Closed Prepaid Cards	These are cards that can only be used for purchases using POS terminals. They cannot be used to withdraw cash and can only be used at a specific group of companies/ entities/ restaurants, such as prepaid cards used at entertainment park/ restaurants.
Closed Prepaid Cards	These are cards that can only be used at one merchant/ company. They cannot be used to draw cash or for e-commerce, and they may be part of a merchant or company closed system.
Service Provider	Any of the entities with which the bank has entered into contract, upon obtaining CBE's approval, to provide all or part of the payment services using prepaid card, provided that such entities deposit amounts in Egyptian Pounds or appropriate guarantees at the bank. A service provider may take deposit cash or make cash transfers to customers as specified by the service provider clause.

Personal Identification Number (PIN)	Personal identification No. used in ATMs also to endorse any financial purchase transaction using a card , which must be placed into the machine to complete the financial transaction.
Secure Code	The code sent to the customer by the issuer bank, whether it be a static or dynamic code sent in an SMS or a token which is an additional security factor used for authenticating transactions when cards are used in e-commerce.
Inherent Risk	Level of risks without taking into consideration any supervisory controls or remedial measures taken by the bank, which consists of the two elements of impact and probable occurrence.
Residual Risk	Risks to which the bank may be exposed after applying remedial controls and measures concerning residual risks.
Business Continuity Plan	Logistic plans on how the bank could recover and regain its vital functions, which were wholly or partially affected (on an urgent basis) within a timeframe specified in advance after catastrophe or service breakdown occurs.
Risk Management	The constant operation for determining, measuring, monitoring and managing exposure to potential risks.
Risk Appetite	The level of risks the bank can bear to achieve its business goals.
Penetration Testing	The manual test tailored to identify the security vulnerabilities points of the system structure or any application environment.

1- Scope of Regulations

1-1
These regulations shall apply over payment services using prepaid card without prejudice to monitory controls on e-banking issued by CBE according to the Circular issued in 2002 and circulars issued afterwards, as well as the regulations and directives concerning the execution of bank transactions, regulations on anti-money laundering and terrorism combating financing issued by CBE, in addition to Customers Due Diligence Procedures issued by the Egyptian Money Laundering Combating Unit (EMLCU), the instructions on internal monitoring of banks issued in September 2014 and the instructions on bank customer rights issued in February 2019.

1-2
These regulations and controls shall be the minimum that must be satisfied for the provision of payment services using prepaid card. The banks must take all necessary measures for the management of risks associated to the provision of this type of banking services.

1-3
These regulations include some general supervisory controls and objectives relating to the continuity of business and the outsourcing and IT risk management. However, the detailed regulations controls these fields shall be issued separately afterwards.

2- Risk Management relating to payment services using Prepaid Card

2-1 Risks associated with Prepaid Cards

The provision of payment services using prepaid card is associated with several risks and benefits at the same time. Although such risks are not new to banks, nonetheless, the provision of payment services using prepaid card could increase the level of risks and may impose new risk management challenges. These risks are outlined hereinafter, for example without limitation:

- Strategic Risks:
  This concerns decision making to provide payment services using prepaid card, the type of services provided and selection of the appropriate time to provide such services. This shall particularly refer to the extent with which the provision or continuity of such services shall be economically efficient, and whether the return on investment would exceed the initial investment and the expenses for the continual provision of these services. Further, bad planning of payment services using prepaid card and making incautious investment decisions may increase strategic risks for banks.

- Operational/ Transaction Risks:
  This concerns risks caused by fraud, or mistakes when carrying out transactions, defects in card functions or other unexpected incidents that may affect the bank's ability to provide the services or that may expose the bank or its customers to financial losses. Although there are risks in all provided products and services, however, the level of risks concerning transactions is affected by the structure of bank measures and transactions. This includes the types of services provided and the degree of complexity of the operations as well as the assisting technical means.

- Compliance/ Legal Risks
  These risks arise as a result of the deployment of payment services using prepaid card and the differences between electronic transactions and non-electronic ones. Regulatory/ legal challenges may include the following:

  - Finalizing an online legal agreement with customers for payment services using prepaid card.

  - The methods used by banks for customer identification and verification, which is deemed one of the legal risks that require setting out adequate controls to mitigate such risks.

  - The bank's legal liability towards customers as a result of the possible breach/ hacking of personal data or any other problems caused by piracy, fraud or other technical failures. The bank shall be responsible for protecting such data from being stolen.

- Banks providing payment services using prepaid card bear higher compliance risks, owing to the changeable nature of technology and monitory modifications addressing problems relating to the provision of these types of services.

- The required compliance documents shall be kept by the bank, relating to records, applications/ software, account statements, disclosures and notices.

- Reputation Risks:
  The level of reputation risks increases with the bank's decision to provide payment services using prepaid card, especially when it comes to more complex transactions. Hereinafter are some of the risks that may affect a bank's reputation when providing payment services using prepaid card:

  - Lack of trust as a result of unauthorized transactions on the card holder's account.

  - Disclosure of the cardholder's confidential information to unauthorized persons or the stealing thereof.

  - Failure to provide reliable services due to the repeated or lengthy breakdown of the system.

  - Complaints by cardholders concerning the difficulty to use payment services using prepaid card or a bank employee's inability to provide the necessary technical support to solve these problems.

  - Misuse of payment services using prepaid card in money laundering transactions.

- Information Security Risks:
  These types of risks arise as a result of an illegal entity's taking advantage of the weak points of the payment services using prepaid card system, which would affect the level of soundness, accessibility and confidentiality of information.

2-2 Responsibilities & Obligations of the Board of Directors & Senior Management

2-2-1 The bank's Board of Directors shall be responsible for ratification of the bank's work strategy and for issuing a clear strategic decision whether the bank should provide payment services using prepaid card or not. The Board of Directors shall particularly satisfy the following conditions:

- Compliance of planned payment services using prepaid card with the bank's strategic objectives.

- Conduction of risk analysis of payment services using prepaid card prior to their launching.

- Setting appropriate measures for identified risk control and mitigation.

- Ongoing monitoring to assess the results of payment services using prepaid card according to the set schemes and objectives.

2-2-2 The Board of Directors and Senior Management should ensure conduction of the risk analysis of payment services using prepaid card as referred to in clause 2-1 and to mitigate such risks by all appropriate means, as set out hereinafter:

2-2-2-1 Effective monitoring of risks associated payment services using prepaid card , including identifying risk management responsibilities, policies and monitory controls:

- The Board of Directors and senior management must ensure that the bank does not issue new payment services using prepaid card nor adopts new technological methods unless the bank has the necessary expertise that would enable it to carry out risk management effectively. The experience of employees and management should be compatible with the technical nature and the level of complexity of the applications and techniques of the payment services using prepaid card.

- The Board of directors and senior management should determine the level of the bank's risk appetite with regard to payment services using prepaid card , while ensuring that risk management operations relating to these services are enlisted among the bank's general risk management methodology. Further, existing policies and operations relating to risk management should be reviewed in order to verify their ability to cover new risks that may arise as a result of payment services using prepaid card. CBE shall be furnished with evidence establishing that such review has taken place upon the commencement of providing such payment services using prepaid card.

- Both internal auditing and compliance departments have to submit a periodic independent and objective assessment to the Board of Directors, the Audit Committee and senior management on the degree of efficiency of the internal controls applied to mitigate risks associated with payment services using prepaid card , including risks relating to technology, money laundering and financing terrorism.

2-2-2-2 Auditing and Ratification of Main Aspects of the Bank's Security Control Process:

- The Board of Directors and top management shall supervise the constant development and maintenance of the security control infrastructure that provides the appropriate protection of the prepaid cards system and data against any internal or external threats. To ensure the efficiency of the security process of payment services using prepaid card , the Board of Directors and top management shall ensure that the following conditions have been met:

  - Identifying clear responsibilities for overseeing the status and management of the bank's security policies.

- To provide the necessary protection to prevent unauthorized access to the computer environment, which contains all the vital systems, the servers, databases, applications and contacts, as well as the security systems of payment services using prepaid card.

- To provide the necessary electronic controls, which could prevent any internal or external unauthorized party from having access to the applications and databases of payment services using prepaid card.

- Regular review of the testing of security measures and systems, such as the regular penetration testing, including the constant follow up of developments in security systems in this field, and to download and prepare software updates and appropriate service parcels and the necessary measures after carrying out the required tests.

2-2-2-3 To set up a comprehensive and sustainable mechanism for conducting due diligences and to monitor outsourcing operations and the bank's relations with other external parties relied upon for the provision of payment services using prepaid card , with special focus by the Board of Directors on the following for example without limitation:

- To have full knowledge of the risks that may occur as a result of entering into any engagement or agency arrangement relating to payment services using prepaid card , and making available the necessary resources required for supervising such arrangements.

- To conduct due diligences on the efficiency and infrastructure of the system and the financial ability of a partner or external party providing the service prior to concluding any engagement or agency agreements.

- To clearly determine the contractual responsibilities of all parties of the engagement or agency agreement, for example, the responsibility to provide and receive information to and from the service provider.

- Engagement and agency contracts shall include a non-disclosure agreement to prevent the disclosure of confidential information to external parties, a service-level agreement, which shall include, for example without limitation: the determination of roles, responsibilities and the required time to provide the service, information concerning escalation and penalties in cases of non-compliance, in addition to clauses for reserving the bank's right to auditing service providers or to rely on ratified audit reports (issued by authorized auditors).

- All systems and operations concerning payment services using prepaid card taking place through appointment, engagement or authorization shall be subject to the risk management system and information security policies that are in line with the bank standards.

- To carry out regular internal and/ or external auditing of transactions taking place through outsourcing or agency arrangements, provided that the scope of auditing shall not be less than that applied for internal auditing.

- To give inspectors from CBE's monitoring and supervision sector access to all auditing and assessment reports.

- To set up appropriate emergency plans for payment services using prepaid card provided by means of engagement or agency.

- Measures for cancellation/ termination of contracts must be effective. Such measures should also ensure the continuity of work and the soundness of the information and its transfer and destruction.

- In spite of the fact that the bank shall outsource some services, yet the bank shall remain fully responsible for prepaid cardholders and for the external parties' abidance by these regulations.

According to clause 3-1, detailed statutory regulations shall be issued regulating outsourcing activities in detail, which shall include detailed supervisory controls and supervisory targets, as well as a list of the systems and services that may be outsourced. Until such regulations are issued, the bank must obtain CBE's prior approval if the bank wishing to outsource payment services using prepaid card or their applications.

2-2-2-4 Top management should ensure that the regularly updated information security policy applied by the bank and ratified by the Board of Directors, covers payment services using prepaid card, which would help identify the required supervisory policies, measures and controls to protect bank transactions from security hacks, and determine individual responsibilities, execution mechanisms and measures that should be taken in case of infringement of these policies or measures.

2-2-2-5 Senior management shall also undertake to promote and streamline the security culture across all bank levels by verifying abidance by high information security standards and streamlining this culture among all bank employees.

2-3 Classification of Prepaid Card Risks

Banks provide different groups of payment services using prepaid card to different categories of customers. Accordingly, they usually do not all bear the same level of inherent risks.

This variety requires that banks adopt security schemes that are comprehensive, yet flexible at the same time, where the security methodology builds on the risk and threat analysis of payment services using prepaid card, while taking into consideration inherent risks to reach the level of residual risks, which fall among the acceptable risk levels for the bank.

2-4 Regulations of Anti-Money Laundering and Terrorism Combatting Financing

- Banks issuing prepaid cards shall satisfy the following conditions:

  - Abide by Law No. 80 of 2002 Promulgating Anti-Money Laundering & its Executive Regulations, bank control regulations on anti-money laundering & terrorism combatting financing issued by CBE, and Customers Due Diligence Procedures issued in March 2019 by EMLCU.

  - Give proper attention as to the nature of service according to the guiding indicators mentioned in clause 7 (guidance indicators to identify suspicious transactions that may include money laundering or financing terrorism) of the bank supervisory controls concerning anti-money laundering and financing terrorism issued by CBE.

  - In case of any suspicious transactions taking place using prepaid cards, they should be reported to the unit of anti-money laundering and terrorism combating financing in accordance with the provisions of Law No. 80 of 2002 on Anti-Money Laundering.

3- Supervisory Controls over payment services using prepaid card

3-1 Issuance of Prepaid Cards

3-1-1
The right to issue payment services using prepaid card shall be restricted to banks authorized to do so by CBE.

3-1-2
The bank issuing payment services using prepaid card, shall develop and run a system for the complete, accurate and continual management of the prepaid cards, which records shall at least indicate the value of the prepaid cards , the cardholder, the service providers and a statement on the balance of accounts of each, as well as the total sum of these balances. This system shall monitor the transactions of payment orders via prepaid cards and shall issue an audit trail on payment orders, while linking the transactions to the cardholders. The system's failure to issue sound reports, whether ratified or not, shall be deemed a violation of these regulations.

3-2 using of Service Provider

3-2-1
The bank may use a service provider to provide payment services using prepaid card after obtaining CBE's consent while paying due regard to the provisions of clause 2-2-2-3. An agreement shall be reached between the bank and the service provider on the operations to be carried out by the service provider, which shall not exceed the following:

3-2-1-1
If the service provider is one of the entities mentioned in clause 3 of the Customers Due Diligence Procedures issued by EMLCU issued in March 2019, the service provider shall:

- Identify and verify the identity of the prepaid card applicant according to the Customers Due Diligence Procedures issued by EMLCU.
- Receive and register application forms submitted for the issuance of cards and any other applications relating to the service.
- Raise awareness and provide guiding information on how to use the card.
- Receive cash deposit (in EGP) from the card users within the limit of the service provider's balance at the bank.

3-2-2
The service provider shall have a good financial position and a good reputation.

3-2-3
The service provider shall open a credit current account at the bank.

3-2-4
The volume of transactions carried out by the service provider shall be restricted to the amount deposited in cash (in EGP) or the bank guarantee (provided that the bank shall periodically assess the guarantees submitted by the service provider, to ensure that the service provider's transactions shall not, at any time, exceed the bank guarantee) in order to transfer same to the cardholders in consideration of cash deposit from them. The service provider may not receive deposits from cardholders without transferring balances to them.

3-2-5
The service provider referred to in clause 1-1-2-3 shall send the prepaid card applicant's identity verification documents to the bank in accordance with the Customers Due Diligence Procedures issued by EMLCU.

3-2-6
The service provider shall set up an appropriate place for carrying out the financial transactions of the service.

3-2-7
The service provider shall provide liquidity to cover the expected cash withdrawing. Should the service provider fail to fulfil this obligation, the penalties mentioned in the contract between it and the bank shall apply.

3-2-8
The bank shall be fully responsible for card holders and shall be held responsible for the service provider's commitment to carry out these regulations, as well as the provisions, controls, regulations and measures that are issued pertaining to anti-money laundering and terrorism combatting financing.

3-2-9
The service provider may not outsource the services for which a contract was signed with the bank. It may not assign or transfer such contract with the bank to others, which this shall be explicitly mentioned in that contract.

3-2-10
The bank shall verify that service providers comply with the payment card industry data security standard PCI DSS.

3-2-11
CBE shall be entitled to inspect any of the bank's service providers and to suspend/ cancel any of their licenses in the event they do not abide by the regulations issued by CBE.

3-3 Management of Prepaid Cards

3-3-1
The bank undertakes to issue prepaid cards upon verifying the identity of the applicant according to the Customers Due Diligence Procedures issued by EMLCU. It shall also abide by Law No. 80 of 2002 on Anti-Money Laundering and Terrorism Combating Financing & its Executive Regulations, Supervisory Controls of Banks on combatting money laundering and financing terrorism issued by CBE.

3-3-2
The bank shall document all data concerning the card issuance time and place, as well as withdrawing and depositing transactions.

3-3-3
The bank shall keep all documents concerning the cards in a safe manner for the set legal periods.

3-3-4
Prepaid cards shall be issued in Egyptian Pounds only. CBE's prior approval shall obtained before issuing any prepaid cards in foreign currency.

3-3-5
Banks must put in place the supervisory measures and controls that would enable them to verify the identity of anyone carrying out an electronic transaction on the prepaid cards and shall verify the identity of the depositor in case of depositing.

3-3-6
Banks shall obtain all the required legal documents to prove authorizing users to carry out transactions on micro enterprise and company cards.

3-3-7
The bank and the service provider shall abide by provisions on confidentiality of accounts as required by Law No. 88 on he Law of the Central Bank, the Banking Sector and Money, and its amendments.

3-3-8
Banks shall carry out the necessary investigations for identity verification of cardholders requesting to make any amendments. This shall also apply to card re-activation and re-issuance of new PINs, in addition to requests for changing contacts such as email addresses, landline No. and addresses. Banks shall further take into consideration applying the following standards when dealing with these applications:

- If the cardholder requests changing his data at any of the service provider's branches or outlets, the necessary measures shall be followed to verify his identity.

- Additional investigation shall be conducted to confirm the cardholder's identity with regard to requests made over the phone "by customers only" to send new security codes or other important documents. An example of additional investigation would be asking questions concerning personal details in general, such as the approximate balance in the card and the last transactions carried out on the card.

3-3-9
The cards must have a smart chip.

3-3-10
Each bank identification No. shall have distinctive encryption keys compliant with the international standards issued by EMVCO.

3-3-11
In case of multi application cards, another consent must be obtained from CBE.

3-3-12
Such cards may be embossed or non-embossed.

3-3-13
The cards must not be activated before they are handed over to customers. They can only be activated after ensuring receiving by the customer. Therefore, the bank must set up a mechanism for verifying customers' receiving of cards.

3-3-14
The maximum validity period of a card shall be five years only.

3-3-15
The bank shall set up a mechanism to ensure that customers are clearly familiarized with all the prepaid card terms & conditions and fees.

3-3-16
Only domestic transfers may be made from prepaid cards. On the other hand, transfers may be made to the card from inside Egypt and abroad according to the transfer regulations mentioned in the Customers Due Diligence Procedures issued by EMLCU.

3-3-17
The bank shall provide customers with a mechanism to see the financial transactions made on the cards, such as mini-statements through ATMs, electronic account statements and printed account statements.

3-3-18
The prepaid card systems may be connected to the bank's different systems, for example without limitation:

- Internet banking system.
- Mobile phone banking system.
- Mobile wallet.

3-3-19
The bank shall set up a mechanism to ensure that a customer receives his card.

3-3-20
Banks may issue co-branded cards with an entity/ authority/ company, whether public or private, where the card would bear the logo of the bank issuing the card and the logo of the other entity/ authority/ company. Such cards shall be subject to the same regulations applied over the aforementioned prepaid cards.

3-3-21
A Personal Identification Number "PIN" must be applied for using these cards as well as a secure code for online transactions.

3-3-22
Based on the bank's assessment of the risks associated with the service and the prepaid cardholder, it shall set a ceiling for the balance, value and No. of daily and monthly transactions on the prepaid cards, as set out hereinafter:

- When a customer's identity is verified according to the Customers Due Diligence Procedures issued by EMLCU:
  - Ceiling of the card balance shall be EGP 20,000.
  - Daily ceiling for withdrawing, transferring and purchasing shall be EGP 12,000 for each bank customer.
  - Monthly ceiling for withdrawing, transferring and purchasing for each bank customer, who is a natural person, shall be EGP 100,000 and, for companies and micro-enterprises, shall be EGP 200,000.
  - The maximum No. of prepaid cards that may be issued by one bank to a person shall be one card.
- CBE Governor may adjust these ceilings and the No. of cards issued by the bank to one person.
- As an exception from the foregoing rule to abide by these ceilings and numbers of cards issued by one bank to one person, shall be the persons who have been verified under the identity verification measures(full KYC), according to the regulations on bank customer identification, issued by the unit on combatting money laundering and financing terrorism of 2011, and its amendments, provided that the bank shall carry out the following:
  - Assessment of risks associated with the service and the use of the cards, and set a ceiling for the balance, value and number of daily and monthly transactions over prepaid cards.
  - Based on the bank's assessment of the risks associated with the service, the bank shall consider to what extent it should be considered a high risk service or not and shall apply strict due diligence measures over the cardholder and his transactions.
  - Special attention shall be given to customers, including the regular monitoring of his transactions, ensuring that there is no suspicion of money laundering, financing terrorism or any other crime.
  - Banks shall notify its prepaid card customers of any high-risk financial transactions or activities taking place over their cards through an alternative automated means (such as SMS or email).

3-3-23
When closing a card, appropriate measures should be taken to ensure that the card's balance is withdrawn, to verify the drawer's identity and to authenticate closing the card account.

3-3-24
Both internal audit and commitment departments should regularly submit an independent and objective assessment to the Board of Directors, the Audit Committee and Top Management on the extent of efficiency of internal controls that are applied to mitigate risks of payment services using prepaid card, including technical risks, and risks relating to money laundering and financing terrorism.

3- 4 Incidents Response and Management

3-4-1

Banks should lay measures to respond to and manage incidents during the provision of services, to ensure immediate reporting and remedying of any security violations, whether they be actual or suspicious, as well as any acts of fraud or any break down/ interruption of payment services using prepaid card, whether during or after work hours. Banks should carry out the following measures, for example without limitation:

- Speedy detection of the source of the incident, and to determine whether it took place as a result of weak points in the bank's security system or not.
- To assess the potential scope of the incident and the extent of its impact.
- To immediately escalate the matter to the bank's senior management if the incident may affect the bank's reputation or cause financial losses.
- To immediately notify the affected victims, as deemed necessary.
- To contain losses concerning bank assets, data and reputation, especially losses relating to customers.
- To collect criminal evidence and to maintain it in a manner that would ensure the monitoring of such evidence in order to facilitate further investigations, to file a court case against card violators and other suspects, as deemed necessary, in addition to following up the incident.

3-4-2

A team should be formed for rapid intervention in order to manage the incident in compliance with the aforementioned measures, provided that this team is granted the necessary authorities to act in emergency cases. The team shall also take adequate training on how to use security tools, to interpret significant relevant data in the audit records, to determine the appropriate measures that should be taken, such as to prevent a certain movement over the network, or to shut down some services.

3-4-3

Banks should set up a record of unexpected incidents relating to prepaid cards and their details, and should prepare a regular report to be presented to top management to take the necessary measures to avoid the repetition of such incidents.

3-4-4

The bank's commitment officer shall be responsible for ensuring that CBE is notified in a sound manner and timing about all of the following cases:

- Any hacking attempts to leak or disclose the identity of the cardholder or identification documents, such as Phishing, Trojans or malware.
- Unauthorized access to the bank's IT system to leak information on the cardholder concerning the payment services using prepaid card.

- Any destructive acts to the data relating to prepaid card systems which may not be recovered.

- Deliberate or accidental complete cessation of payment services using prepaid card for a period exceeding the recovery time objective (RTO) set by the bank.

- Any internal cases of fraud relating to payment services using prepaid card.

3-4-5
CBE and the cardholders must be notified publicly about any changes in the service tariff.

3-4-6
The bank shall submit monthly reports to CBE, covering the volume of transactions, the No. of issued cards, the No. of service providers, the volume of daily transactions of all kinds, and any other data required by CBE.

3-4-7
The standards shall be applied over the prepaid card system operator as a whole or any operator in charge of the partial operation of the system. CBE shall be entitled to inspect any part of the prepaid card system to ensure compliance with the standards and specifications issued by CBE. Any impediment of CBE's mission to this end shall be deemed a violation of these regulations by the relevant bank running that system.

3-5 Performance Considerations and Ensuring Work Continuity

3-5-1
Banks should provide payment services using prepaid card around the clock, while ensuring the service is carried out for customers with the proper speed as mentioned in the service terms and conditions, while taking customers' expectations into consideration.

3-5-2
Banks should lay standards for the monitoring and evaluation of performance levels of payment services using prepaid card. They should take the necessary measures to ensure that payment services using prepaid card and internal systems are capable of dealing with the volume of expected operations and the future growth of such type of services.

3-5-3
- In case of any beak-down of the service, the work continuity plan should outline specific steps for resuming or recovering payment services using prepaid card. Such steps shall be identified based on previously determined RTO & RPO.

- There should be recoverable data-backup and an alternative work plan for emergencies.

- The work continuity plan of payment services using prepaid card should be capable of dealing with cases of outsourcing services (to contractors).

3-6 Information Confidentiality and Soundness

3-6-1
The provision of payment services using prepaid card involves the exchange of confidential information, such as card No. and financial transactions…etc. over the bank's intranet and the internet. Therefore, it is essential that banks adopt appropriate means to maintain the confidentiality and soundness of circulated information over the bank's intranet and internet.

3-6-2
Tokens shall be used to protect the confidentiality and soundness of sensitive information. Hence, banks should select an encryption technology that suits the sensitivity and importance of the information as well as the required level of protection. Within this context, it is always recommended that banks adopt internationally recognizable encryption technologies where their points of strength undergo comprehensive tests. Banks should apply sound practices for management of the necessary encryption keys in order to protect these keys.

3-6-3
Banks should also apply other controls besides tokens/ encryption, to maintain the confidentiality and soundness of the information circulated over the payment services using prepaid card, which shall include the following for example without limitation:

- The regulations and due diligences enlisted in the prepaid card applications in order to ensure the sound settlement of customers' balances and in order to verify the soundness of the data transferred between the different systems.

- To monitor unusual transactions, including suspicious transactions in payment services using prepaid card or records that are suspected to be manipulated, as outlined in clause 4-2.

3-6-4
Banks should ensure the encryption of the data of prepaid cards up to servers used for carrying out a payment order.

3-6-5
The bank should separate tasks to ensure that none of the bank's internal employees can carry out or hide any unauthorized act, which may include, without limitation, management of the card account, to carry out transactions, maintain and administrate encryption keys of the system, system administration and system operations. The bank shall also tailor measures in a manner that would ensure that one employee alone could not start, approve or carry out any dealings over the system, which could support a fraudulent act or hide details concerning such dealings.

3-6-6

All authorization checks and regulations control transfers should take place over the server, in other words through the bank's back office before carrying out the required transaction (for instance, transfers should take place reversely in case the user's authority is not authenticated, which could enable the user to add funds to the card account instead of deduct amounts).

4- Customer Security and Other Risk Controls

4-1 Service Provision Contract/ Service Application Form

A bank shall clearly determine all rights and obligations between it and its customers in the contract concluded for the issuance of prepaid cards. Banks shall comply with instructions on the protection of bank customer rights issued in February 2019. The contract shall satisfy the following conditions at least:

- The contract shall be drafted in a clear and accurate manner that can be easily understood by any customer, while avoiding the use of any words or expressions that can bear multiple meanings.
- The obligations of each of the bank and the cardholder shall be demonstrated in cases of violation of any of the contract terms.
- The contract shall contain specific and clear provisions, which shall include the following at least:
  - Customers shall be advised if the service is down due to scheduled maintenance.
  - The level of privacy of the customers' data and to what extent it can be accessible internally or outside the bank, shall be demonstrated, in accordance with the supervisory instructions issued by CBE or laws regulating this matter, and the instructions on the protection of bank customer rights issued in February 2019 shall be abided by.
  - A detailed illustration shall be made of the steps that should be taken by a cardholder for activation of the card, or in cases when the card is suspended or re-activated, while demonstrating the different means of requesting suspension of the card.
  - The ability to cease use of the service if abused/ misused by the cardholder.
  - The bank shall develop a mechanism to study complaints. The service subscription contract shall explicitly state the means of raising a complaint to the bank, and the maximum period to be taken by the bank for looking into the complaint.
  - In case there are any disputed financial transactions or complaints by cardholders, dispute resolution shall be subject to fixed regulations announced to the cardholder. These regulations must be stated in the contract concluded between the cardholder and the bank, while noting that the bank records shall be conclusive evidence, that there is no defect in the bank system and that there are complete records of the dealings, subject of the dispute.
  - It should be clearly noted that competent Egyptian laws, their executive regulations and supervisory regulations and instructions shall govern the services provided by the bank to its customers. Further, disputes shall be settled in Egypt.
  - The cardholder's responsibility to safeguard his password/ PIN and to report the loss of his card immediately shall be clearly stressed. A copy of the contract form (terms & conditions) shall be published on the bank's website.

- If the system operation is terminated by the bank or in any other case leading to suspension of the service, the bank must fulfil its obligations for its cardholders, including recovery of the balance in the cards according to the contract terms between the bank and the cardholder as soon as possible.

- The bank shall ensure the customer's physical signature of the contract. An exception to this clause may only be made upon receiving CBE's written approval.

4-2 Detection of Unusual Activities

4-2-1
Banks should set effective measures for constant monitoring to ensure the rapid detection of any unusual or suspicious transactions taking place over prepaid cards, that may be part of a fraud. Such measures shall, particularly, be able to detect the following cases:

- Multiple transfers of funds using prepaid cards to the account of another beneficiary within a short period of time, especially if such transferred amounts are close to the permitted ceiling, in addition to the sudden increase in the amounts transferred to the cards of other beneficiaries.

- Change of the cardholder's address used for bank correspondences, followed shortly by activities that may indicate probable illegal operations, such as a request to send some important documents, such as the PIN to this new address.

4-2-2
The monitory mechanism should be capable of sending out speedy warnings to the monitoring and follow up officers overseeing the payment services using prepaid card in case of any suspicious transfer of funds that may be part of a fraud, in addition to any unusual activities carried out over the prepaid cards. In such cases, banks should hold investigations with these account holders to which the transactions or activities are made as soon as possible and should notify the competent authorities.

4-2-3
Customers shall be immediately notified if any unusual activity that may be a fraud takes place over their cards.

4-2-4
The bank shall apply specified and ratified procedures to deal with cases of fraud.

4-2-5
The bank shall advise its customers of the procedures they should take if they find out they have lost their card/ a fraudulent act took place, which shall include, for example without limitation, contacting the customers service center, reporting to the bank premises/ the service provider..etc.

4-2-6
The bank shall lay the appropriate procedures to issue another card in replacement of the customer's lost card/ suspend the card, while ensuring that the balance in the lost card is transferred to the customer after verifying the customer's data.

5- License Procedures

1- Banks wishing to provide payment services using prepaid card to their customers shall submit an application for approval by CBE, while indicating the cards to be issued and their details.

2- Banks that already obtained licenses to carry out payment services using prepaid card prior to the issuance of these regulations, shall adjust their statuses and satisfy the following requirements:

- Adjust their statuses according to a set time schedule in order to address the gaps between the bank's current status and the standards and controls issued by CBE, within three months at the most as of the date of the issuance of these regulations. The banks undertake to adjust their statuses according to CBE's regulations within a grace period of three months at the most as of the date of submitting the status adjustment plan.

- Should a bank not adjust its status during that fixed period of time, this might lead to cancellation of the payment services using prepaid card license granted to the bank.

Annex A- Cases and regulations for Appointing Prepaid Card Service Providers

A bank shall appoint a service provider to apply customer identification and verification measures as per clause 5 of the Customers Due Diligence Procedures issued by EMLCU, in the following cases:

1- The service provider is a mobile network company operating in Egypt in accordance with Telecommunications Law No. 10 of 2003, whether the service is provided by one of its fixed or moveable branches or outlets, provided that customer identification and verification shall take place by one of the company employees.

2- The service provider is a post office affiliated to the Egypt national Postal Authority (Egypt Post), provided that the customer identification and verification measures shall be applied by one of the Egypt Post's employees.

3- The service provider is a company, association or a civil society organization licensed to exercise micro-financing by the Egyptian Financial Regulatory Authority (FRA) in accordance with Law No. 141 of 2014 and the decrees issued for the execution thereof, provided that the following conditions are met:

- The entity must have a valid commercial register and tax card, in cases of companies, or statutes ratified by the Ministry of Social Solidarity in cases of associations and civil society organizations.
- A letter from FRA establishing its consent, provided that such entity is the service provider.
- The entity's services shall be restricted to its customers receiving micro-finance, which shall be in compliance with the provisions of Law No. 141 of 2014 and the decrees issued in execution thereof.

4- The service provider is a governmental authority or a public sector unit, through competent departments, after obtaining CBE's consent to this end.

5- The service provider is another entity other than those mentioned in the preceding clauses, provided that the following conditions are met:

- The entity has a valid commercial register and a valid tax card.
- If the entity provides a service through one of its outlets at another entity, the other entity musty have a valid commercial register and a valid tax card.
- The bank shall render the owners and managers of the entity subject to the bank's customer due diligence procedures and shall collect any information it deems necessary about them.

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

- The terms & conditions contained in the contract concluded with that entity shall stipulate the setting up of systems and measures that would ensure that its employees and those of its outlets, enjoyed high efficiency and transparency standards. Such systems and measures shall at least ensure inquiring about employee's former positions and obtaining criminal clearance statements.

In all the previous cases, the following regulations shall be applied:

1- The bank shall specify customer identification and verification measures in line with the provisions of clause 5 of Customers Due Diligence Procedures issued by EMLCU. 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.

2- The bank shall lay appropriate measures to regularly verify compliance of the customer providers with customer identification and verification procedures. In the event there are any material or repeated violations in this regard, according to the standards laid 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- The contract signed between the bank and the service provider should enlist 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 application of these procedures.

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

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 this 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 operations that may be carried out.

The bank shall abide by any materials that shall be issued by EMLCU in this regard.

Annex B Comparison between the Different Types of Prepaid Cards

Type	Definition	Cash Draw/ Transfer	Purchase via POS
Open Card	Can be used at any merchant without being specified	Permitted	Permitted
Semi-Open Card	Can be used at any merchant without being specified (such as gift cards)	Unpermitted	Permitted
Semi-Closed Card	Can be used at specified merchants (such as cards for specific restaurants)	Unpermitted	Permitted


PREPAID CARD
PREPAID CARD
PREPAID CARD PREPAID CARD
Enter
Clear


PREPAID
PREPAID CARD
1234 5678 4587
CARDHOLDER NAME
10/18
10/25

البنك المركزي المصري
CENTRAL BANK OF EGYPT

54 شارع الجمهورية، وسط البلد، القاهرة،مصر
54 El Gomhoreya St., Downtown, Cairo, Egypt
info@cbe.org.eg | **16777**
P.O.Box: 11511 :صندوق بريد