Technical Payment Aggregators & Payment Facilitators Regulations

In the Arab Republic of Egypt

Technical Payment Aggregators & Payment Facilitators Regulations

In the Arab Republic of Egypt


البنك المركزي المصري
CENTRAL BANK OF EGYPT

Table of Contents

Introduction

These regulations have been prepared to cope with the fast developments taking place in collection, bill payments and the payment for services, in addition to the need for the services of technical payment aggregators and payment facilitators, which can give many merchants and companies access to financial and technical services. These regulations also illustrate the appropriate means of contracting to help the deployment of e-Payments services across alternative delivery channels, which would greatly contribute to acceptance of the different means of payment instruments by these categories of companies and merchants, and would, in turn, ensure realizing safe tangible steps for all stakeholders in the field of e-Payments.

General Definitions

Technical Payment Aggregator

A company with financial solvency that provides technical services to its sub-merchants on behalf of the bank through the alternative delivery channels of the technical payment aggregator, which includes providing e-payments services for paying bills/services, which roles shall include the following for example without limitation:

- To set up a technical platform for collecting the value of bills/ services for sub-merchants and link them to electronic collection methods.
- To provide the bank with information on the sub-merchants that shall be enlisted therewith.
- To provide the means of contracting with sub-merchants according to the bank's terms and conditions.
- To provide the required technical support to sub-merchants on behalf of the bank.
- To raise the necessary awareness among sub-merchants with regard to the financial services provided thereby on behalf of the bank.
- To make available all necessary reports to sub-merchants on all transactions carried out through technical payment aggregator channels.

Payment Facilitator

A company with financial solvency that provides financial and technical services through alternative delivery channels of its sub-merchants with which contracts have been concluded on behalf of the bank for the provision of e-Payments services, which roles shall include the following for example without limitation:

- To set up a technical platform for sub-merchants and link them to electronic collection methods.
- To set up intermediary systems that provide added value services to sub-merchants and link them to electronic collection methods.
- To provide the bank with information on the sub-merchants through which electronic collection methods shall take place.
- To contract with sub-merchants on behalf of the bank for the provision of electronic collection methods.
- To receive financial settlements from the bank with which a contract has been concluded on behalf of its enlisted sub-merchants.
- To carry out financial settlements for enlisted sub-merchants on behalf of the bank.
- To provide the necessary financial support to its enlisted sub-merchants on behalf of the bank.
- To raise necessary awareness among its enlisted sub-merchants with regard to financial services provided thereby on behalf of the bank.
- To make available all necessary reports to its sub-merchants on all financial transactions carried out through same.

Sub-merchant of Technical Payment Aggregator	Sub-merchants that have a valid legal status which enters into contract with the technical payment aggregator and the bank (according to the mentioned means of contracting) to provide services for settlement of bills / services for customers through the alternative delivery channels of technical payment aggregator & payment facilitators, provided that the following is fulfilled by the sub-merchant: • It has a bank account to which the value of bills / services are collected or transferred. • An actual premises inside Egypt. • Clear contact information (a valid phone number / email address)
Sub-merchant of Payment Facilitator	Sub-merchants that have a valid legal status which enters into contract with the payment facilitator to provide e-Payments services to its customers through its alternative delivery channels, such as the company website, its mobile application, its branches… etc.
Alternative Delivery Channels	Delivery channels that allow e-Payments collection services by customers, which shall include the following for example without limitation: • POS. • E-commerce. • Mobile wallet.

1- Scope of Regulations

- These regulations and controls are the minimum that must be followed by banks for using technical payment aggregators and payment facilitators. Hence, all banks should not suffice with such regulations as they must ensure that all necessary measures are taken for ensuring risk management relating to these types of bank services.

- These regulations controls using technical payment aggregators and payment facilitators only, without prejudice to the supervisory controls over e-banking transactions issued by CBE, the directives and rules regulating bank transactions, controls on anti-money laundering and terrorism combatting financing issued by CBE and due diligence regulations with regard to customers issued by the anti-money laundering and terrorism combatting financing unit.

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

The bank's Board of Directors shall be responsible for ratification of the work strategy prepared by its Senior Management and for issuing a clear strategic decision whether the bank should deal with technical payment aggregators and payment facilitators or not. The Board of Directors shall particularly satisfy the following conditions:

- Compliance of plans to use the services of technical payment aggregators and payment facilitators with the bank's strategic objectives.
- Performing risk analysis for these services.
- Setting appropriate measures for risk control and mitigation.
- Setting appropriate measures for risk monitoring and the mitigation of identified risks.
- Ongoing monitoring to assess the results of reliance on technical payment aggregators and payment facilitators according to the set goals and objectives.
- To conduct regular inspection missions on technical payment aggregators and payment facilitators.

  To conduct the necessary due diligences on the efficiency, infrastructure and financial ability of the technical payment aggregators and payment facilitators before entering into any agreement, and to develop an inclusive and sustainable mechanism to conduct due diligences and monitor such service providers, including the following for example, without limitation:

  - Technical due diligence.
  - Financial due diligence.
  - Reputation inquiry.
- The bank shall lay a risk policy for technical payment aggregators and payment facilitators and shall conduct risk studies relating to the following:
  - Refunds.
  - Fraud.
  - Disputes.
  - Bankruptcy.

3-Risks relating to the Provided Services

The provision of electronic collection services through technical payment aggregators and payment facilitators are associated with many risks and benefits at the same time. Perhaps these risks are not new to banks, nonetheless, electronic collection services via technical payment aggregators and payment facilitators may increase the level of risks, and may also impose new risk management challenges. These risks may include the following for example without limitation:

3-1 Strategic Risks:

- This concerns making the decision to provide electronic collection services through technical payment aggregators and payment facilitators, the type of services provided and the selection of the appropriate time to provide such services. This particularly refers to what extent such services are economically efficient.

3-2 Operation/ Transaction Risks:

- This concerns risks caused by fraud, refund, disputes, mistakes when carrying out the transactions, defects in the work system of technical payment aggregators and payment facilitators or even the bank system, or other unexpected acts that may affect the bank's ability to provide the services or that may expose the bank or its customers to financial loss. Although there are risks in all products and services that are provided, however, the level of risks concerning transactions is affected by the structure of the bank measures and operations. This includes the types of services provided and the extent of the complexity of the operations as well as the assisting technical means.

3-3 Compliance/ Legal Risks

- These risks arise as a result of the deployment of electronic collection services via technical payment aggregators and payment facilitators. Regulatory/ legal challenges may include the following:

  - In light of the bank's compliance with Law No. 88 of 2003 of the Central Bank, Banking Sector and Monetary System, it should lay measures and controls to maintain the confidentiality of customers' data and accounts, so as to ensure the management of increased the risks relating to electronic collection services services provided by technical payment aggregators and payment facilitators, in addition to the bank's legal responsibility towards its customers as a result of the possible hacking of confidential data or any other problems resulting from piracy, fraud or other technical failures, based on which banks should strive to protect such data from being stolen.

- Banks providing electronic collection services through technical payment aggregators and payment facilitators bear higher compliance risks, owing to the changeable nature of technology and having to monitor modifications addressing problems relating to the provision of these types of services.

- Banks should maintain the required compliance documents relating to records, applications/ software, account statements, disclosures and notices.

- Banks should identify and assess risks relating to money laundering and financing terrorism, which may arise from electronic collection services through technical payment aggregators and payment facilitators and e-payments. Such assessment should be completed before the launching of the electronic collection services services via technical payment aggregators and payment facilitators. If the service already exists at the bank, this would require conducting a re-assessment as soon as these Rules, according to the monitory requirements contained herein, as well as the diligence measures concerning customers issued by the unit of combatting money laundering and financing terrorism.

3-4 Reputation Risks:

- The level of reputation risks increases as a result of the bank's decision to provide electronic collection services services through technical payment aggregators and payment facilitators, especially when it comes to more complex dealings. Hereinafter are some of the risks that may affect a bank's reputation when providing electronic collection services services through technical payment aggregators and payment facilitators:

  - Disclosure of confidential information to unauthorized persons or the theft thereof.

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

  - Complaints concerning the difficulty to use electronic collection services services via technical payment aggregators and payment facilitators or an employee's inability to provide the necessary technical support to solve these problems.

4- Regulations of Anti-Money Laundering, Terrorism Combatting Financing and Information Security

4-1
Abidance by Law No. 80 of 2002 Promulgating Anti-Money Laundering & its Executive Regulations, supervisory controls for of Anti-Money Laundering, Terrorism Combatting Financing and Information Security, client identification Regulations issued in 2011, diligence measures concerning customers using mobile wallet payment services issued in 2016 and all future amendments thereto.

4-2
To give proper attention as to the nature of the service in order to detect suspicious operations that may include money laundering or financing terrorism according to bank control regulations of Anti-Money Laundering, Terrorism Combatting Financing and Information Security issued by CBE in 2008.

4-3
In case of any suspicious dealings in the services provided by technical payment aggregators and payment facilitators, they should be reported to the unit of of Anti-Money Laundering, Terrorism Combatting Financing and Information Security in accordance with the provisions of Law No. 80 of 2002 on Anti-Money Laundering.

4-4
To abide by any instructions issued by CBE afterwards concerning technical payment aggregators and payment facilitators.

4-5
Any hacking of any data of concerning technical payment aggregators and payment facilitators, must be immediately reported to CBE's information security department at **cbe.infosec@cbe.org.eg**, the cyber security sector at **csirc-team@cbe.org.eg**, and the monitory and control sector.

5- Development of Information Security Policy

5-1
Senior management shall ensure that the information security policy adopted by the bank, which is ratified by its Board of Directors and which is regularly updated, addresses electronic collection services through technical payment aggregators and payment facilitators. This shall contribute to identifying the necessary monitory policies, measures and controls to protect the bank operations from any security infringement or violation. Individual responsibilities will also be determined, in addition to specifying execution mechanisms and measures to be taken in cases of violation of such policies and procedures.

5-2
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.

6- General Rules for Banks using Technical Payment Aggregators and Payment Facilitators

6-1

Contracts with technical payment aggregators and payment facilitators shall include the following:

6-1-1

To clearly determine the contractual liabilities of all parties of the engagement/appointment, partnership or agency agreements. For instance, the responsibilities for providing and receiving information to and from technical payment aggregators and payment facilitators.

6-1-2

Non-disclosure agreement to protect confidential information of external parties and an agreement on the level of services, which includes for example without limitation: determination of roles & responsibilities, the required time to carry out the services, as well as information on means of escalation and penalties in cases of non-compliance, in addition to provisions reserving the bank's right to auditing the services or to rely on ratified audit reports (issued by accredited auditors).

6-1-3

The contract between the bank and the technical payment aggregators and payment facilitators shall allow for the possible immediate suspension/ Termination of any sub-merchant's and the bank shall set the mechanism to stop any sub-merchant immediately

6-1-4

All systems and operations concerning electronic collection services through outsourcing, engagement or authorization of technical payment aggregators and payment facilitators shall be subject to the risk management system and information security policies in line with the bank standards.

6-1-5

All due diligence and assessment reports shall be made available to the inspectors from CBE's monitoring and supervision sector.

6-1-6

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

6-1-7

Technical payment aggregators and payment facilitators shall not be authorized to sub-contract other companies (external parties) to carry out the works assigned thereto by the bank by virtue of this contract, without first obtaining the bank's approval, and the works assigned by the technical payment aggregators and payment facilitators to the sub-contractors must be specified.

6-2
General Rules

6-2-1
The bank shall carry out regular internal and/ or external auditing of the operations, which shall cover, at least, the same internal auditing works of the bank.

6-2-2
The bank shall develop the appropriate emergency plans for electronic collection services by technical payment aggregators and payment facilitators.

6-2-3
Technical payment aggregators and payment facilitators shall carefully inspect the papers of sub-merchants, which shall be enlisted with them according to the conditions contained in the approval, and to the bank's conditions.

6-2-4
The bank shall receive data and documents on each contracted sub-merchant according to the bank requirements; and technical payment aggregators and payment facilitators shall obtain the approval of the bank prior to enlisting the sub-merchant on the list of technical payment aggregators and payment facilitators providing their services.

6-2-5
The bank should put in place a mechanism that allows it to have complete control over accepting or stopping the settlement of the sub-merchants' total daily proceeds enlisted with the technical payment aggregators and payment facilitators based on the "value of the bank guarantee provided by the technical payment aggregators and payment facilitators at the bank".

6-2-6
The bank shall at least develop an internal system that would enable it to carry out constant monitoring of operations taking place through the technical payment aggregators and payment facilitators, which shall include the following:

- Before activating the service, the bank shall ensure that none of the sub-merchants are blacklisted.

- To ensure that there are no suspicious acts relating to money laundering, financing terrorism or any crime, according to the law on anti-money laundering promulgated by Law No. 80 of 2002.

6-2-7
The bank shall apply a mechanism that would enable it to stop electronic collection services operations by sub-merchants of technical payment aggregators and payment facilitators online.

6-2-8
The bank shall inspect transactions carried out by sub-merchants on a daily basis without relying on the technical payment aggregators and payment facilitators to do this.

6-2-9
The bank shall put in place a system for auditing the transactions of technical payment aggregators and payment facilitators, which would enable it to check, match and audit all transactions taking place through them by all their sub-merchants instantly/ daily.

6-2-10
The bank shall ensure that the technical payment aggregators and payment facilitators have in place a system for inspecting and monitoring transactions of sub-merchants affiliated thereto in order to monitor their transactions and inspect them diligently.

6-2-11
The bank shall launch regular inspection missions over the premises and systems of the technical payment aggregators and payment facilitators to verify compliance with work regulations along with the regulations issued by the bank, which must be provided for in the contract concluded between the bank and the technical payment aggregators and payment facilitators.

6-2-12
The bank shall set clear rules for the resolution of disputes that may arise between the parties of the system according to the delivery channels that are used.

6-2-13
The bank shall ensure that the technical payment aggregators and payment facilitators provide a customers service centre to reply to any inquiries and to raise awareness among sub-merchants concerning the following:

- How to use the system, extract required reports and have access to data on specific transactions.
- Fraudulent acts and how to study transactions.
- Objections, the mechanism used, and required documents for such transactions.

6-2-14
The sub-merchants enlisted with the technical payment aggregators and payment facilitators shall be prohibited from carrying out the following activities:

- Virtual / Crypto Currency.
- Network/ pyramid scheme marketing.
- Sale/ purchase of securities.
- Filing and file sharing.
- Dating Mobile apps/ websites.
- Sale and purchase of gold, jewellery and precious stones.
- Gambling and lottery, including casino games, races and the like.
- Crowd funding.

6-2-15
None of the companies or activities requiring CBE's prior approval shall be enlisted with the technical payment aggregators or payment facilitators without first obtaining CBE's approval.

6-2-16

With regard to the payment facilitators, the bank shall verify the following:

- That the sub-merchant is a valid legal entity according to the regulations on checking customer identities issued in 2011 as well as mobile payment regulations issued in 2016 and all further amendments thereto, while verifying the following:
  - It has an actual premises in Egypt.
  - It has clear contact information (phone No. inside Egypt/ email address).
  - It has a website/ mobile app (if any, according to the service provided).

- The payment facilitator shall transfer the electronic collections of the sub-merchants according to the service level agreed upon with he sub-merchants enlisted therewith, provided that the electronic collections shall be transferred on the second business day or within 3 business days at the most as of the ssdate of the financial transaction, provided that the bank lays the mechanism that would guarantee this takes place.

- The bank shall maintain a bank guarantee submitted by the payment facilitator to secure the transactions implemented through it, which guarantee shall be equivalent to or more than the value of the electronic collections by the payment facilitator during three business days, provided that such guarantee shall be periodically re-assessed. However, it is not permitted, in any case whatsoever, that the value of the electronic collections by the payment facilitator exceed the guarantee kept at the bank.

- The bank shall ensure that the settlement account of the payment facilitator only concerns its sub-merchants' electronic collections, and that such electronic collections are not used in any of the payment facilitator's other businesses.

- To regularly monitor the financial transactions concerning the services provided by the payment facilitator to sub-merchants according to the agreed upon level of services.

- It is essential that the bank show all transactions taking place through the sub-merchants according to the following details (name of payment facilitator, name of sub-merchant).

- The bank shall carry out the regular inspection works of the sub-merchants' alternative delivery channels and shall satisfy the following conditions, for example without limitation:

  - That there is a separate description of goods and services provided by the sub-merchants.
  - That the sub-merchants provide an actual product/ service and not a fake one.
  - That there are clear contact information (phone No./ email address) in Egypt.
  - That there is a clear refund policy.
  - That there is a clear policy for product delivery and arrival time.

- Transactions of payment facilitators and their sub-merchants shall be restricted to authorizations or settlement-clearing in Egyptian Pounds only and not in any other currency.

- Limits and rules governing sub-merchants listed with payment facilitators:

  - Sub-merchants engaged in this system are those enlisted under the category of small merchants whose online proceeds from all alternative delivery channels used do not exceed three million Egyptian pounds annually, which ceiling may be modified by the CBE Governor.

  - In the event the electronic collections of any sub-merchant exceeds three million Egyptian Pounds annually, the bank shall terminate it from the payment facilitator model and shall contract it directly according to the regular contract procedures carried out by the bank with any company. In addition, a tri-partite contract can be concluded between the bank, the sub-merchant and the payment facilitator, to use it, in this case, as a provider of technical services, while abiding by all rules issued in this regard.

  - Governmental organizations shall not work under the model of payment facilitators.

  - A payment facilitator shall not be enlisted as a sub-merchant with another payment facilitator.

  - Donation organizations shall not be listed as sub-merchants with payment facilitators model.

6-2-17

Concerning technical payment aggregators, the bank shall abide by the following:

- Contractual terms of technical payment aggregators and sub-merchants enlisted therewith:

  - A direct contract shall be concluded between the sub-merchant, the bank providing the service, and the technical payment aggregator.

  - Or the sub-merchant shall issue an authorization to the technical payment aggregator (upon its signature authentication by the sub-merchant's bank) for entering into contract with banks on behalf thereof, without the technical payment aggregator's account acting as a party or liaison in the transfer process, at any time.

  - Or a contract shall be concluded between the technical payment aggregator and the sub-merchants, provided that a letter of understanding is issued by each sub-merchant addressed to each acquiring bank.

- It is essential that the bank keep a bank guarantee submitted by the technical payment aggregator to secure the transactions carried out through it, which guarantee shall be equivalent to or more than 50% of the value of the electronic collections by the technical payment aggregator daily, provided that such guarantee shall be regularly re-assessed, and in no case whatsoever, can the value of the proceeds of the transactions collected by the technical payment aggregator exceed double the value of the guarantee kept at the bank.

- The technical payment aggregator shall send a daily file to the bank, containing all successful transactions that shall be settled in favour of its sub-merchants

  The bank shall settle the daily proceeds in the bank's suspense account such that the technical payment aggregator shall not be capable of making any transactions (draws, deposits or transfers) to or from this account.

- The bank shall carry out a daily comparison/ matching of the value of invoices/ services against the data provided by the technical payment aggregators, such that the bank shall settle the daily electronic collections into the account of each sub-merchant of the technical payment aggregator. In case of any discrepancies, the bank's settlement shall be the prevailing statement. The bank should develop a mechanism to be applied with technical payment aggregators to settle any such discrepancies.

- Before activating the services for sub-merchants of technical payment aggregators, the bank shall verify that each sub-merchant has valid legal standing according to the identification rules issued in 2011, as well as mobile wallet payment rules issued in 2016 and all future amendments thereto, while satisfying the following conditions:

  - To specify the types of invoices/ services that the technical payment aggregators shall render available for collection by their sub-merchants.

  - To specify the sub-merchant's bank account number to which the value of invoices paid shall be transferred.

  - To have an actual premises in Egypt.

  - To have clear contact information (phone No. inside Egypt/ email address).

- The transactions of the technical payment aggregator and its sub-merchants, shall be restricted to cases where there are authorizations or settlement- clearing in Egyptian Pounds only and no other currency without first obtaining CBE's approval.

- Regulations governing sub-merchants enlisted with technical payment aggregators

  - Governmental organizations and authorities shall not work under the model of technical payment aggregators without first obtaining CBE's approval.

  - A technical payment aggregator shall not be enlisted as a sub-merchant with another invoice collector except in the cases specified by CBE.

  - In the event the bank wishes to use the services of technical payment aggregators through alternative distribution channels of sub-merchants, another approval must be obtained from CBE.

  - Donation organizations shall be collected through this model, provided that the following conditions are satisfied:

    - The donation organizations must have a valid permit to collect funds.

    - Any donations collected after the expiry of the permit shall be held/ set aside until the permit is renewed.

    - Donations may not be collected in foreign currency unless there is authorization to do so in the donation organizations permit.

    - The bank must lay an appropriate mechanism to prevent the acceptance of donations from abroad should this be specified in the donor's fund collection permit.

7- Information Confidentiality and Soundness

7-1
The provision of electronic collections services through technical payment aggregators or payment facilitators involves the exchange of confidential information. Therefore, it is important that banks adopt appropriate means to maintain the confidentiality and soundness of circulated information.

7-2
encryption 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 in order to protect them.

7-3
Banks should also apply other controls besides encryption, to maintain the confidentiality and soundness of the information circulated over electronic collection services, which shall include the following for example without limitation:

7-3-1
The rules and audits enlisted in the electronic collection applications used in order to ensure the sound settlement of the balances of transactions and in order to verify the soundness of the data transferred between the different systems.

7-3-2
To monitor unusual transactions, including suspicious transactions in the used electronic collection services or records that are suspected to be manipulated.

7-3-3
Banks should ensure the encryption of payment transactions starting from the distribution channel used for carrying out the transaction up to the servers through which the payment order is made.

7-3-4
The bank should apply a separation policy for tasks to ensure that none of the bank's internal employees can carry out and hide any unauthorized act, which may include, without limitation, management of the account of the technical payment aggregator or the payment facilitator, and to carry out transactions, maintain and administrate the system encryption keys and undertake system administration and system operations, according to the following:

- Not to allow any one employee alone to open an account for a technical payment aggregator or a payment facilitator, not may any one employee authorize or cancel this, without engaging other bank employees, in order to ensure the employee acts in a sound manner.

- The bank should tailor measures regarding transactions of technical payment aggregators and payment facilitators so as to ensure that no one carries out any transactions solitarily over the system, which could help in any fraud or in hiding any details concerning such transactions.

7-3-5
All authorization checks and rules regulating electronic collection should take place through the server, i.e. in the bank's back office systems before carrying out any transaction on the bank system.

8- Detection of Unusual Activities

8-1
Banks should set effective measures for constant monitoring to ensure the rapid detection of any unusual or suspicious transactions that may be part of a fraud.

8-2
The monitory system must be able to send out speedy warnings to competent officers in order to monitor and detect any unusual activities. In such cases, banks shall verify these unusual activities as soon as possible and shall notify the competent authorities of same.

8-3
The bank shall apply specific ratified procedures for dealing with fraudulent acts.

9- Raising Awareness among Sub-Merchants

9-1
Due to the possible risks that may occur in cases where sub-merchants of technical payment aggregators or payment facilitators are unfamiliar with the necessary procedures and guidance concerning these services, or in cases where they misunderstand such procedures, therefore, technical payment aggregators and payment facilitators must pay special attention to raising awareness among sub-merchants, by providing them with clear and easily understandable advice on the necessary security precautions that should be followed when dealing with electronic collections and the significance of abiding by such guidance/ precautions.

9-2
Banks, technical payment aggregators and payment facilitators must develop effective means and channels to report to sub-merchants and raise their awareness on security precautions that must be followed by them. The bank and the technical payment aggregators & payment facilitators may benefit from several means, such as websites and promotional publications, as well as through front desk officers working at the bank or with technical payment aggregators and payment facilitators when they communicate with sub-merchants to stress the significance of abiding by certain basic precautionary measures.

10- License Procedures

10-1
Banks wishing to enter into contract with technical payment aggregators and payment facilitators shall submit an application to obtain CBE's consent, upon satisfying the following paper requirements at least :

10-1-1
List of the delivery channels the banks wishes to use through technical payment aggregators and payment facilitators.

10-1-2
Detailed work flow to be followed for each delivery channel separately.

10-1-3
Plan of the bank as well as the technical payment aggregators and payment facilitators to enlist sub-merchants, such as, for example without limitation, delivery channels to be used, the No. of sub-merchants to be contracted, and the targeted No. and value of transactions to be collected).

10-1-4
A statement indicating any case of complete or partial non-abidance of technical payment aggregators and payment facilitators by contractual regulations issued by CBE, provided that all issued regulations must be satisfied within 6 months at the most from the date thereof.

10-2
To pass the necessary tests according to the alternative delivery channels to be used by technical payment aggregators and payment facilitators and to furnish CBE with evidence of passing such tests.

10-3
The bank shall not launch the service with technical payment aggregators and payment facilitators before furnishing CBE with a penetration test report on the actual work productions, including the following, for example without limitation:

- Merchant plugins.
- Software development kit- SDK.
- Application programming interfaces.

This would indicate that there are no weak points with high or medium level risks, based on which CBE's approval would be granted to activate the service, provided that the report would be submitted within three months at the most as of the issuance of the approval, while noting that it is essential to take these tests regularly and to provide the bank with the penetration test report which is conditional for license renewal.

10-4
If the bank wishes to add any new delivery channels to technical payment aggregators and payment facilitators, it must obtain a new approval from CBE to this end.

10-5
The Bank shall provide the Sector of Payment Systems and Information Technology at CBE with quarterly reports (in both soft and hard copy), including the following information at least:

- The No. of sub-merchants enlisted with technical payment aggregators and payment facilitators according to the alternative delivery channels.

- Total No. and value of transactions of sub-merchants of technical payment aggregators and payment facilitators.

10-6
Complete abidance by any reports or regulations issued by CBE pertaining to technical payment aggregators and payment facilitators.

10-7
The bank undertakes to activate the services of technical payment aggregators and payment facilitators within six months as of the date of obtaining the license from CBE.

10-8
CBE shall be entitled to inspect any part of the system to verify compliance with standards and specifications set out by CBE. Any attempt to impede CBE's such mission shall be deemed a violation of these rules by the relevant bank running the system. CBE may impose appropriate penalties according to the provisions of Article 135 of Law No. 88 of 2003 on the Central Bank, Banking Sector and Monetary System and the amendments thereof.

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