Guidance on

Combating Financial Fraud in the National Payment System

Central Bank of Jordan
Oversight and Supervision on National Payments System Department
May, 2023

This Guidance entitled "Combating Financial Fraud in the National Payments System" was prepared by the Studies and Policies Division/ Oversight and Supervision on the National Payments System Department at the Central Bank of Jordan. It was prepared by Eng. Iman Bani Atteyah, Studies and Policy Specialist, and Ibrahim Al-Ramadan, Head of the Studies and Policies division in editing, reviewing and supervising.

Moreover, for the purposes of consultation, this Guidance was shared with and presented to each of the Compliance Monitoring Committee for electronic payment and money transfer companies, and the Committee for Follow-up on Financial Fraud Cases in the financial sector, as well as to all banks operating in the Kingdom in cooperation and coordination with the Association of Banks in Jordan.

Central Bank of Jordan
Oversight and Supervision on the National Payments System
Department of Studies and Policies Department
Tel: 0096264630301
Fax: 0096264600521
P.O. BOX 37 AMMAN 11118 JORDAN
Website: www.cbj.gov.jo
Email: studies.oversight@cbj.gov.jo

Contents

Introduction

Recent decades have been characterized by the growth of technological development and the rapid pace of innovations that target all aspects of life, including the economic one. Financial institutions have increasingly relied on technology and its innovations to deliver their financial and banking services, according to new business models based on internet platforms and mobile applications. This has opened the way for them to provide huge business opportunities, especially for startups, including establishing business or banking relationships with customers electronically, thereby expanding their business scope and contributing to the creation of a highly competitive environment in their markets.

With the increasing reliance of financial institutions on electronic means for onboarding customers and providing financial and banking services and products to them, the prevalence of electronic financial crimes has also risen. These crimes have become a strong threat to financial institutions, encompassing financial losses, information security risks, data theft, and operational risks associated with cyberattacks. Such attacks can disrupt the financial institution's systems and deny services to customers. Moreover, these financial crimes give rise to other risks, including reputational risks and potential legal implications.

Financial institutions may be exposed to new risks due to the adoption and use of modern technologies and their innovations, apart from the ill-considered and uncontrolled use of information and communication technology, which could lead to the disruption of necessary financial and banking services, whether for national or international financial systems. This undermines security and confidence in the financial and banking system and its integrity, and endangering financial stability. Since financial institutions are not immune to the risks of electronic financial crimes, efforts must be combined to identify, understand and evaluate the risks of these crimes in an appropriate manner, leading to the development of the necessary measures to prevent, mitigate and recover from them if they occur.

Fraud is considered one of the most important challenges facing financial institutions and their customers alike, as its consequences are dire. It may pose significant harm to financial institutions, extending beyond mere financial losses to potentially damaging their reputation, the impact of which may be transmitted to the entire financial and banking sector, in addition to reducing confidence among customers and the public in adopting and using electronic means to carry out banking and financial operations, including electronic payments and transfers.

The danger of fraud stems from its potential to extend beyond individual financial institution and impact the entire sector, as previously indicated. Add to that, the changing dynamic of fraud tactics, as it is rapidly evolving and adapting to technological developments and changes that occur in the financial and banking sector's business models, particularly on the payments side. Despite the development and implementation of protection mechanisms and controls by financial institutions to combat fraud, there is a steady increase in successful fraudulent incidents within the payments sector.

Assessing the potential losses that may result from a successful fraud operation on the financial institution's services is often challenging, as the matter goes beyond financial losses that can be easily estimated to other losses that are difficult to estimate, such as the impact on reputation and competitive value in the market, and the decline in customer confidence. This situation may lead to the possibility of activating money laundering and terrorist financing crimes that affect the integrity of the financial system as a whole, not to mention any penalties or fines that may be imposed by the Central Bank due to non-compliance with regulations and legislation, if this is proven.

In response to this, financial institutions are compelled to increase their investments in the development and utilization of systems and programs essential for monitoring, combating, and deterring fraud, which may be less costly compared to the expenses incurred when attempting to recover from fraud incidents if they were to occur.

The purpose of this Guidance

This Guidance comes out of the Central Bank of Jordan's keenness to enable and assist companies - including banks and exchange companies - licensed by the Central Bank of Jordan (Hereinafter referred to as "the Central Bank") to practice the activities of providing electronic payment services and managing and operating electronic payment systems to manage the risks associated with financial fraud within the National Payments System efficiently and effectively, regardless of whether it originates from employees within the Company, with their assistance, from customers, or from third parties. The Guidance also aims to enhance sound understanding and good knowledge of the appropriate measures and procedures concerning preventing and combating financial fraud, dealing with them appropriately, and monitoring emerging and innovative techniques employed in fraudulent cases. Additionally, it enables companies to tailor these procedures and measures to align with the nature of their work and activities. Furthermore, it empowers them to enhance their capacity in developing and implementing necessary counter-fraud programs in accordance with a risk-based approach.

This Guidance encompasses comprehensive guidelines for establishing robust governance practices in combating fraud incidents that a company may exposed to, including defining clear roles and responsibilities for all supervisory and functional layers within the organization. These roles entail developing and implementing preventive, detective, and corrective controls aimed at detecting, combating, and recovering from fraud cases in a timely manner. This begins with the Board of Directors and extends to Senior Executive Management, including internal auditors, compliance officers, and risk management staff, reaching to the rest of the employees in the Company, as well as the role and responsibilities of clients in preventing and detecting fraud, as their actions can either contribute to or impede the success of fraudulent operations. Furthermore, the Guidance outlined procedures for disseminating and promoting awareness about combating fraud and fostering a good culture in particular.

It should be noted that the procedures and measures outlined in this Guidance serve as minimum guidelines for combating financial fraud that companies can

leverage and utilize as a foundation for developing their own policies, work procedures, and control mechanisms. Companies are encouraged to implement additional measures and procedures based on the outcomes of their risk assessments, taking into consideration the unique nature of their business and activities.

Legislative framework:

The development of this Guidance comes from the authorities granted to the Central Bank of Jordan under the provisions of Article (4/b) of its Law No. (23) of 1971, and its amendments. This Article defines the tasks entrusted to the Central Bank, which include organizing and developing the National Payments System to ensure the provision of safe and efficient payment, clearing, and settlement systems in the Kingdom, in order to achieve its objectives, which included contributing to achieving banking and financial stability in the Kingdom, as outlined in paragraph (a) of the aforementioned Article. Also, based on the Central Bank's supervisory and oversight role over the National Payments System, as stipulated in Article (50/a) of the above law.

Moreover, this Guidance aligns with legislative requirements concerning combating fraud and managing related risks. In addition, to enhance the companies' ability to comply with the provisions of the applicable legislation without any deficiencies or weaknesses in their procedures taken in this regard. The most prominent legislation governing companies in relation to combating fraud includes the following:

A. The provisions of Article (93/a) of the Banking Law No. (28) of 2000 and its amendments stipulated that "If a bank learns that the execution of any banking transaction or the receipt or payment of fund is related to any crime or illegitimate act, the bank shall immediately notify the Central Bank accordingly".

B. According to the provisions of Article (5/f) of the Electronic Payment and Money Transfer Bylaw No. (111) of 2017 issued pursuant to the provisions of Articles (21) and (22) of the Electronic Transactions Law No. (15) of 2015; companies are

mandated to establish clear and efficient rules and systems to respond to customers' inquiries and complaints, protect their interests, resolve disputes that may arise from the services provided to them, and procedures for reporting thefts, losses or data breaches due to the use of services and refunding money.

C. The provisions of Article (35) of the Electronic Payment and Money Transfer Bylaw No. (111) of 2017 oblige payment service providers to ensure that the credential data used for the purposes of authenticating the customer's identity are not available to others, and to provide appropriate means to enable the customer to report the loss or theft or breach of personal credential data.

D. Companies are also obligated, based on the provisions of Article (36) of the Electronic Payment and Money Transfer Bylaw No. (111) of 2017, to notify the Central Bank, relevant authorities, and other involved parties of any cases of penetration or fraud that the Company or any third party contracting with may be exposed to immediately upon their occurrence.

Disclaimer

This Guidance has been issued to provide companies engaged in providing electronic payment services and/or the managing and operating electronic payment systems with guidance to combat financial fraud. It is important to note that this Guidance is not mandatory unless the Central Bank's orders specify otherwise. In case of any conflicts between the procedures outlined in this Guidance and the existing legislation, the provisions within the legislation will prevail. However, it is essential for companies to inform the Central Bank about any such conflicts to address them appropriately.

Scope of application

This Guidance has been issued to companies licensed by the Central Bank- including banks and exchange companies - to practice the business of providing electronic payment services and managing and operating electronic payment systems, for the

purposes of relying on it in combating financial fraud that may affect any of the National Payment System components. It is important to note that companies must adhere to the existing legislation concerning fraud and must not violate its provisions. Furthermore, the Central Bank has the authority to direct this Guidance to other financial institutions that fall under its oversight and supervision through special orders issued specifically to this purpose.

First: Introduction to Financial Fraud

1. Financial Fraud Concept

The term of fraud is commonly used to describe a wide range of misconduct, including theft, corruption, embezzlement, bribery, forgery, misrepresentation, collusion, money laundering, and concealment of material facts, often involving illegal acts of deception, concealment, or breach of trust; with the aim of achieving personal gain for the benefit of an individual or a third party.

Fraud is defined as “The use of deception to obtain an unlawful benefit” or “any practice that involves the use of deception to obtain, directly or indirectly, some form of financial benefit for the perpetrator, or facilitate it for others, leading to a loss for the party who was defrauded”.

On the Jordanian legislator level, the provisions of Article (417) of the in force Penal Code stipulated that fraud is: "Whoever makes another person deliver to him/her any moveable or immoveable property or any documents which includes an undertaking or a remission from dep’t and he/she takes control of it through deception". Through this text, fraud can be defined as wrongful appropriation of movable or immovable funds or bonds through deceptive tactics and means, which coerce the other party into complying and surrendering them.

For the fraud crime to be committed, the offender must perform a material act of appropriating the money of others by fraudulent means, in addition to the criminal intent, wherein the will of the offender is directed towards unlawfully seizing the money of others through the fraudulent means employed.

Fraud is based on dishonesty and deception, The Jordanian legislator, in Article (417) of the in force Penal Code, has defined the fraudulent means; through the use of deceptive means which makes the victim falsely believe the existence of a false project or instance or to raise the victim's hopes that he/she will gain profits or that he/she will retrieve the amount of money taken from him/her, or the existence of a dep't bond, through the disposition of a moveable or immoveable property while knowing that he/she has no capacity to do so, and through the use of false name or a wrong capacity.

In a similar vein, electronic fraud can be defined according to Article (11) of the Arab Convention on Combating Information Technology Offenses as "The intentional and unlawful infliction of harm to beneficiaries and users with the aim of fraudulent activity, pursuing illicit interests and gains for the perpetrator or third parties, through actions such as introducing, modifying, deleting, or blocking information and data, disrupting the functionality of operating systems and communication networks, attempting to disable or alter them, or disabling hardware, software, and websites".

Financial Fraud and Money Laundering:

Fraud is considered one of the original offenses associated with money laundering, and there is a significant connection between money laundering and financial fraud. Typically, perpetrators of fraud often engage in money laundering to conceal the illicit origins of the funds obtained through financial fraud. Therefore, there is an overlap in the measures taken to combat financial fraud on the one hand, and measures to combat money laundering on the other hand.

2. Financial Fraud Common Types

In light of the technological development that the world has witnessed in recent decades, which has resulted in the provision of financial services using these technologies, consequently, individuals and companies increasingly rely on electronic payment processes. As technical means for accessing financial services

and products continue to evolve, financial fraud methods are also evolving and taking on various forms over time. Nonetheless, their ultimate objective remains consistent to deceive individuals with the intention of gaining access to their financial and personal information, leading to the theft of their money and savings.

However, regardless of the multitude of fraud methods, it is crucial to recognize that exercising caution and vigilance is the most effective way to protect oneself against financial fraud. In the following section, we will explore key forms of fraud and protection against them.

In the same context, fraud methods in electronic payments exhibit dynamic characteristics. However, they can be traced back to several primary forms. A single instance of financial fraud may involve the utilization of multiple forms from these primary forms, which we outline as follows:

Social Engineering:

Social engineering fraud is a generic term that refers to fraudulent methods that criminals use to exploit a person's trust in order to directly obtain money or confidential information that will enable them to commit a subsequent crime. Criminals use social engineering tactics because it is usually easier to exploit an individual's natural tendency to trust, instead of discovering ways to attack the Company's systems or devices directly.

Although social media is the preferred channel in this form of financial fraud, social engineering attempts can be made through many electronic and non-electronic means, including email, SMS, and phone calls in addition to social networking sites, and any channel used to communicate with clients that can be exploited by an attacker with varying degrees of sophistication required to carry out the attack.

Among the forms of social engineering in financial fraud is Phishing, and it is a fraudulent method in which the criminal sends a fraudulent message that tricks the recipient into disclosing his/her personal information. The information they request may include payment card details, bank account details, electronic

payment accounts, or various other personal information. It often comes in three types:

- **Email Phishing:** The most common form of phishing attack is carried out via emails, and this type of attack usually involves a fraudster sending an email telling the recipient that their account has been hacked, and that they need to reset his/her password. The objective of email phishing is to deceive the recipient into willingly disclosing his/her login credentials or other sensitive information required by the scammer to carry out his malicious attack.

- **Vishing**: This type of phishing occurs through voice calls. The recipient receives a phone call informing him that his payment card has expired, and they need to reveal his banking credentials to ensure they it is properly reactivated. An example of vishing involves the fraudster contacts the victim claiming that he is one of the Company's employees, creating a sense of urgency by claiming there is an emergency situation that could result in the loss of his money, and then offers him assistance, and the victim just has to verify his credential information, and thus the fraudster can obtain this credential for use in carrying out a transaction through the channel (On-line Banking) or any form of misuse.

- **Smashing**: A type of phishing attack that employs short text messages (SMS) to target unknown victims. The techniques used here are very similar to how an email phishing attack is carried out; where the recipient receives a text message informing him that his account (eg internet banking) has been compromised, and he need to share his current login information to access the account, once the scammer has the login data, they can change the password and prevent the victim from accessing the account.

  The target of the fraud here may be the Company's customer, and he may be the Company's employee who is being exploited to access the Company's systems and data and obtain financial resources directly through carrying out payment operations through the Company's systems, or even disrupt the Company's systems entirely. In such instances, the Company becomes vulnerable to a

security breach and must take appropriate measures to address and rectify the breach promptly.

Customer Identity Theft:

In this type of fraud, the fraudster leverages the customer's identity to initiate a payment, in many instances of this fraud, the initial point of entry for the fraudster is through various forms of phishing attacks aimed at obtaining the victim's online banking credentials. Once the fraudster gains access to these credentials, they proceed to withdraw funds through card payment transactions.

An individual's personal data can be used, and stealing his identity to be used in registering and opening an account with a company. Therefore, it is crucial for companies to exercise due diligence to verify and authenticate the customer registrations, this includes ensuring that the person is who's claiming to be indeed, and that no impersonation or falsification of information has occurred, since the accuracy and truth of all subsequent financial transactions of the registration process, will depend on the accuracy of the registration process.

Merchant Identity Fraud

Much like customer identity fraud, merchant identity fraud involves criminals creating a fraudulent merchant account after illegally obtaining company identification information, and the fraudster uses this newly created "business" to charge commissions to customers' credit cards. Subsequently, the fraudster terminates the account and walks away, leaving behind a trail of chargebacks, customer complaints, and fraud reports.

In addition to the several types of fraud, payment card fraud is constantly evolving, as new technologies drive cybercriminals to develop their methods. It is almost impossible to encompass all these methods in a single list, but there are two main categories:

- **Card Non-Present Fraud**: this is the most common type of fraud and occurs when the cardholder's information is stolen and used illegally without the need for the physical presence of the card. This type of fraud typically occurs online,

and it could be resulted from phishing emails sent by fraudsters impersonating trusted institutions, aiming to steal personal or financial details through deceptive links.

- **Card Present Fraud**: it often takes the form of stealing card information using an electronic device to fraudulently clone the data. While this type is less common nowadays, caution is still necessary, as the deceitful merchant passes the card through a device that stores the card information, this information is then used in any purchase, with the charges being billed to the cardholder's account.

Secondly: Corporate Governance Framework

It is incumbent upon companies to be able to combat financial fraud cases from all sources and address them in a timely and effective manner, within levels of effectiveness and efficiency. This requires establishing a comprehensive and effective governance framework that defines the level of authority, nature of roles, and scope of responsibilities towards implementing the Company's policy in combating financial fraud, in accordance with applicable legislation. The clearer and more comprehensive the delineation of authority, roles, and responsibilities for all supervisory, managerial, and operational levels within the Company, the more it contributes to ensuring the effective implementation of the Company's plans and programs in combating financial fraud.

In order to ensure the implementation of sound corporate governance practices, companies must consider the following requirements when developing and establishing a governance framework specifically for combating financial fraud:

A. Company should establish a dedicated Counter-Financial Fraud Policy covering all its sources, or include the necessary procedures and requirements to combat financial fraud within its internal policies. These policies should clearly define the authorities, roles, and responsibilities related to combating fraud.

B. Company should identify, assess, and understand the risks of financial fraud it may exposed to. It is crucial to adopt a risk-based approach in dealing with and

combating financial fraud cases. This includes incorporating the requirements for combating financial fraud within the Company's overall risk management strategy or comprehensive risk management framework, in order to mitigate the potential levels of financial fraud risks and the associated impacts in case of their occurrence.

C. The Company should establish a dedicated organizational unit responsible for the management of combating financial fraud. The Company can have an independent unit specifically dedicated to carrying out this function or establish a division within the Compliance or Risk Management Unit. The decision on the appropriate structure should be based on the size of the Company's operations, the diversity of its services, the nature of its business, and the level of complexity involved.

D. In order to enhance the governance of its fraud risk management, the Company should establish a committee that is emanated from the Board of Directors to oversee the management of financial fraud cases and the outcomes of their investigations. The tasks of the committee emanated from the Board of Directors can be delegated to the Compliance Committee or the Risk Management Committee.

Furthermore, the responsibility for combating financial fraud lies with all employees of the Company at various functional levels, alongside the Company's Board of Directors. The authorities, responsibilities, and roles should be as follows:

1. Board of Directors

The Company's Board of Directors bears the overall responsibility for overseeing and supervising the efforts to combat financial fraud within the Company, encompassing all its sources. Within this scope, the minimum tasks and responsibilities of the Board of Directors include:

A. Adopting a Counter-Financial Fraud Policy and reviewing it whenever any changes occur, ensuring the policy's suitability for the financial fraud risks within the Company, whether it is a standalone policy or part of other Company's policies.

B. Periodically monitoring and evaluating the effectiveness of the Counter-Financial Fraud Policy to ensure its proper implementation. This includes verifying that all financial fraud cases encountered by the Company have been promptly addressed and managed by Senior Executive Management. Additionally, evaluating the degree of effectiveness with which the Company is managing financial fraud risks at least once a year.

C. Adopting an official document that approves the establishment of a permanent and effective organizational unit within the Company responsible for the function of managing financial fraud operations. This organizational unit can be either an independent unit itself or a division that is structurally subordinate to the Compliance or Risk Management Unit within the Company, as practically feasible and according to the circumstances.

D. Adopting a comprehensive framework for managing financial fraud risks or incorporating them within the overall enterprise-wide risks framework in the Company, and developing key strategies for managing these risks, ensuring that the Company is capable of consistently responding to potential financial fraud risks, reducing the likelihood of such risks occurring, and effectively managing them within a risk-based approach.

E. Ensuring the availability of sufficient financial resources and qualified human resources for the Counter-Financial Fraud Unit, and accurately defining its responsibilities and authorities. This includes granting the Unit the necessary authority to conduct investigations into financial fraud cases involving employees at all levels within the Company, access all necessary information and documents required to carry out its duties, while ensuring the confidentiality requirements are upheld. Additionally, considering subjecting the Unit's activities to regular review by the Company's Internal Audit Function.

F. Holding regular meetings at least quarterly, or as necessary, to discuss financial fraud cases the Company has been exposed to -including attempted financial fraud or potential cases- and the methods used, relevant statistics, presenting the outcomes and assessing the actual or expected impact, the measures taken for immediate reporting of such cases to the Central Bank and other relevant competent authorities, as well as the corrective actions and recommended control measures proposed by the Counter-Financial Fraud Unit, and implementing a mechanism to monitor the implementation of these corrective actions and approved control measures.

G. Reviewing and discussing the Counter-Financial Fraud Annual Report, and ensuring the implementation of all recommendations contained therein in an appropriate manner and time.

H. Taking necessary measures to enhance the values of integrity, transparency, and sound professional practices within the Company in a manner that makes combating financial fraud a fundamental objective that must be achieved, including creating a conducive environment within the Company to foster a culture of combating financial fraud, deterring it, preventing it, and reporting it easily and in a way that guarantees the scope of preservation on confidentiality.

The Board of Directors may choose to delegate the tasks and responsibilities outlined in paragraphs (B), (E), (F), (G), and (H) above, in addition to reviewing the Counter-Financial Fraud Policy and financial fraud risk management procedures, ensuring their effectiveness, and providing necessary recommendations regarding these matters to an independent committee established for this purpose or to the Compliance Monitoring Committee (if exist) or the Risk Management Committee.

2. Counter-Financial Fraud Committee

In the event that the Board of Directors decides to proceed towards the governance of financial fraud risk management by establishing a committee emanated from it,

or assigning this task to the Compliance Committee or the Risk Management Committee, the Committee's duties and responsibilities shall include the following:

A. Performing the specific tasks and responsibilities assigned to the Board of Directors within paragraphs (B), (E), (F), (G), and (H) of item (1) above.

B. Reviewing the Counter-Financial Fraud Policy, including ensuring its alignment with other policies in the Company, particularly the Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) Policy, and the overall Risk Management Framework in the Company. Additionally, reviewing the financial fraud risk management procedures and the preventive, detective, and corrective control measures to ensure their adequacy and effectiveness, and reporting the findings and recommendations to the Board of Directors.

C. Reviewing the results of the Financial Fraud Risk Assessment process, including ensuring that the Company has identified and properly assessed the potential risks, and developed the necessary procedures and control measures in a manner that result in making the residual risks acceptable in accordance with the Company's Risk Management Policy and its risk appetite, and reporting the findings and recommendations regarding this matter to the Board of Directors.

D. Follow-up on investigations in financial fraud cases, whether resulting in financial losses or not, as well as following up on reports related to such cases with relevant competent authorities.

E. Identifying the vulnerabilities that contributed to the occurrences of financial fraud and ensuring the implementation of necessary measures and control mechanisms to address them and prevent their recurrence. This includes identifying the reasons behind any delays in detecting financial fraud incidents that the Company has encountered (if applicable).

F. Follow-up on cases reported to the Central Bank, the Anti-Money Laundering and Counter-Terrorism Financing Unit, and other relevant competent authorities (law enforcement agencies) regarding any proven financial fraud cases that the Company is exposed to, whether it is internal or external fraud,

including those affecting the Company's clients or any third-party contracted with it, and in accordance with the provisions of the legislation in force.

G. Submitting the Committee's recommendations and reports periodically or as needed to the Board of Directors, ensuring that these reports include the following:

1. Details of the financial fraud cases that the company was exposed to, including for example the following:

   - Total number of financial fraud cases (and their values), whether detected or reported.
   - Mechanisms used to carry out the financial fraud cases.
   - Investigation outcomes of the financial fraud cases, including the status of the financial fraud case.
   - Vulnerabilities that were exploited to carry out financial fraud cases.
   - Financial loss that the Company will incur (if any), as well as any other tangible or intangible losses.
   - Average time taken to detect and handle financial fraud cases, along with the reasons for deviations from the target in achieving this.
   - Number of cases that have been resolved, and those still under investigation and review.
   - Corrective or preventive measures implemented to prevent the recurrence of such cases in the future.

2. The results of financial fraud risk assessment operations include, for example, the following:
   - Results of identifying and assessing financial fraud risks.
   - Control measures effectiveness and adequacy in combating financial fraud cases.
   - Performance results for control indicators and suspicious scenario for detecting and uncovering financial fraud cases.
   - Results of implementing the awareness and education plan regarding the risks of financial fraud.

- Indicator of the Company employee's commitment to the procedures for combating financial fraud.
- Results of evaluating access control lists and their effectiveness in combating internal financial fraud.
- The adequacy of the administrative and disciplinary measures taken for internal financial fraud cases.

H. Ensuring the implementation of necessary awareness programs to promote combating financial fraud culture at all functional levels within the Company, including awareness programs designed for customers.

I. Collaborating with other committees emanating from the Board of Directors to exchange necessary information to carry out its tasks.

J. Any other tasks assigned by the Board of Directors.

In order to enable the Counter-Financial Fraud Committee to effectively carry out its tasks and responsibilities, it requires the Board of Directors to develop and approve the necessary arrangements that granting the Committee the right to have direct communication with all employees in the Company, ensuring unrestricted access to all documents, records, disclosures, and devices. in addition to enabling the Committee to seek external consultations to assist and advise in the execution of its tasks, and to address any unresolved issues between the Counter-Financial Fraud Unit and other organizational units, including the Company's General Manager, with the aim of enabling the Counter-Financial Fraud Unit to carry out its tasks.

3. Senior Executive Management

Senior Executive Management in the Company bears full responsibility for implementing the necessary measures to combat financial fraud in all its forms. In

order to achieve this, they are expected to fulfill the following minimum tasks and responsibilities:

A. Managing and organizing the Counter-Financial Fraud Function by establishing the organizational unit concerned with that, nominating/appointing its director/manager, providing it with qualified and appropriate human resources based on competence and eligibility criteria. Additionally, allocating the necessary financial resources to enable it to carry out its tasks, including covering the necessary training needs for its employees continuously and providing the supportive electronic information systems for it.

B. Laying down a Counter-Financial Fraud Policy, approve it from the Board of Directors, and take necessary measures to ensure its implementation and adherence. Additionally, review and update it periodically and whenever necessary, and circulate it across all organizational units and employees in the Company to comply with it. This includes reporting any detected or suspected financial fraud cases to the head of the Counter-Financial Fraud Unit through dedicated communication channels prepared for that purpose. This ensures the implementation of the necessary procedures and controls to detect and address financial fraud cases or suspicions, whether originated internally or externally to the Company, and handle them promptly and appropriately, while verifying the adequacy of these procedures and controls.

C. Developing at least an annual program to manage financial fraud risks in collaboration with the Counter-Financial Fraud unit. The program should encompass the identification, assessment, and determination of financial fraud risks from all sources. It should also include the formulation of corrective plans in the event of any deficiencies in the necessary control procedures to combat potential financial fraud operations and ensuring their implementation.

D. Establishing adequate procedures to ensure that all functional levels within the Company provide the necessary capabilities to the employees of the Counter-Financial Fraud Unit, enabling them to carry out their assigned tasks efficiently and effectively within a framework of trust and harmonious relationships.

Particularly, this applies during their investigation processes of financial fraud cases and their access to the information and documentation necessary to execute their duties.

E. Determining the reporting channels, whether to the Board of Directors, the Central Bank, or any other relevant competent authorities, regarding any instances of financial fraud that the Company or any third parties it contracts with may encounter. Additionally, defining the reporting procedures to the Anti-Money Laundering and Counter-Terrorist Financing Unit in cases where financial fraud operations are suspected to be linked to money laundering or terrorist financing.

F. Developing and ensuring the implementation of educational and awareness programs aimed at all supervisory and functional levels within the Company, starting from the top management and cascading down to the base (Tone at The Top). These programs aim to emphasize the importance, duties, and responsibilities of combating financial fraud operations, as well as reporting and deterring them.

4. Counter-Financial Fraud Unit

As previously mentioned, it is essential for the Company to establish an organizational unit responsible for the Counter-Financial Fraud function. In this regard, the Company may opt for an independent organizational unit dedicated to perform this function, or it could create a division responsible for it, reporting either to the Compliance Monitoring Unit or the Risk Management Unit. The decision on the most suitable approach should be made based on the Company's business size, the diversity of its services, the nature of its operations, and the complexity level involved.

The organizational unit responsible for counter financial fraud tasks, in general, takes charge of assisting the Senior Executive Management at the Company in managing, monitoring, and combating financial fraud risks. Additionally, it carries out the following tasks:

A. Proposing policies, executive plans, operational procedures, and control measures necessary for the Company to combat financial fraud, as well as reviewing and evaluating them periodically and updating them wherever necessary.

B. Using electronic control systems to monitor, detect, and mitigate financial fraud operations, whether from inside or outside the Company, periodically measuring the effectiveness and efficiency of these systems and committing to updating the scenarios and warning indicators for potential financial fraud detection in line with the evolving methods employed in such fraudulent activities. Taking into consideration that these systems should include the following at a minimum:

1. Scenarios and warning indicators based on clear procedures for financial fraud cases.
2. Analyzing customer behavior across all available channels to detect unusual activities related to financial fraud.
3. Developing special scenarios to monitor the accounts of the Company's employees and analyzing their behavior.

C. Investigating potential financial fraud cases against the Company or taking necessary actions in the event the Company is exposed to any fraudulent operation (whether internal or external), including but not limited to:

1. Investigating financial fraud cases committed by any of the Company's employees, or cases that the Company is exposed to by external parties. Given that a committee should be formed within the Company, led by and including members from the Counter-Financial Fraud unit, to carry out the investigation tasks for financial fraud cases, while ensuring the avoidance of conflicts of interest during the formation of this committee.
2. Tracking the processes and exchanging relevant information concerning any financial fraud cases in which the Company is involved, including its customers, in accordance with the provisions of the legislation in force.

3. Freezing the suspected funds involved in a financial fraud case based on a legitimate request from the competent authorities.

4. Promptly and without delay, notifying the Central Bank and other relevant competent authorities (law enforcement authorities) of all financial fraud cases (whether internal or external) immediately upon occurrence or discovery, in which the Company or any of its executives are involved, regardless of whether they have been settled or have not resulted in financial losses.

5. Notifying the Central Bank about all cases in which the Company or any of its executives are not involved, but the Company is responsible for taking necessary legal actions, including taking the decision of whether to report or not to report to other relevant competent authorities (law enforcement agencies). This should be done according to the advice of its legal counsel for each case, and in accordance with the provisions of the relevant legislation.

6. Notifying the Central Bank should be independent of the notification process to other relevant competent authorities, such as law enforcement agencies. The notification should include details such as date of occurrence, involved parties, relevant organizational units within the Company, corrective measures taken, any incurred losses, and the methods used. Additionally, the Central Bank should be subsequently provided with information indicating the notification to other relevant competent authorities and the date of such notification.

7. Notifying the Anti-Money Laundering and Counter-Terrorist Financing Unit in accordance with the specific procedures, channels, and mechanisms established, and in consistent with the requirements of Anti-Money Laundering and Counter-Terrorist Financing Law No. (20) of 2021.

8. Reviewing the policies and operational procedures to identify deficiencies that may have caused or contributed to the occurrence of financial fraud, and

enhancing control measures to prevent the recurrence of financial fraud cases.

9. Collecting the necessary data, information, and documents to support administrative, disciplinary, or other actions, as well as judicial prosecution and attempting to recover funds related to the financial fraud cases.

D. Applying enhanced due diligence procedures specified for combating money laundering and terrorist financing operations concerning financial fraud cases according to the nature of the suspected activities. These procedures shall be implemented in the following cases:

1. When there is a suspicion of financial fraud.
2. When there is a doubt about the authenticity of documents provided by customers or employees.
3. When receiving a correspondence related to suspicions of financial fraud, whether involving Company's employees, customers, financial institutions, third parties, or any other parties.
4. When an alert or warning indicator appears in the electronic monitoring system.
5. When determining the beneficiaries of the funds resulting from financial fraud operations whenever possible.

E. Identifying, evaluating, and documenting potential financial fraud risks related to the Company's activities and operations, including those associated with the development of new products or services, including new mechanisms for service delivery or those that may arise from the use of emerged technological advancements or under developments with regard to both current and new products. Additionally, assessing risks associated with third parties the Company intends to contract with, especially those assigned sensitive tasks, according to well-studied principles, and quantitative and qualitative measurement methods within the scope of collaborative work with relevant organizational units within

the Company. Furthermore, proposing control measures to effectively limit and mitigate these risks to an acceptable manner.

F. Implementing the annual program for financial fraud risk management in collaboration with all organizational units within the Company, in a manner that considers the following within the program:

1. Identifying potential financial fraud risk from all sources, defining and assessing them.
2. Ensuring compliance with the approved Counter-Financial Fraud Policy, including third-parties adherence, through conducting tests to assess the adequacy and suitability of internal controls implemented to manage financial fraud risks within the Company.
3. Developing corrective action plans in case of any deficiencies in the necessary procedures and control measures to combat potential financial fraud cases, and ensuring their efficient and effective implementation.

G. Follow-up on the observations received in reports from the Central Bank, other competent authorities, external auditors, internal audit unit, and any other relevant supervisory entities within the Company related to financial fraud cases, and taking necessary actions accordingly.

H. Disseminating and promoting awareness regarding financial fraud methods to both the Company's clients and employees on an ongoing basis. This includes preparing informative guidelines or brochures and conducting training programs for the Company's employees on topics related to financial fraud risks and prevention, emphasizing the values of integrity and ethical conduct among employees in a manner that makes combating financial fraud a fundamental and integral objective.

I. Continuous review of reports issued by relevant international organizations regarding combating financial fraud and benefiting from the recommended measures and best practices implemented in this regard.

J. Immediate reporting to the Senior Executive Management (as appropriate) regarding any of the following cases, provided that the senior executive management should commit to submitting a copy of these reports to the Board of Directors or its emanating committee that undertakes financial fraud risk management tasks (if applicable) immediately:

1. Any fraud incidents the Company has been exposed to, including investigation outcomes, failures, or deficiencies that led to or contributed to the success of the financial fraud, along with recommended corrective actions and measures.
2. Identification of a new fraud typology or phenomenon and the recommended measures to protect the Company from being exposed to.
3. Identification of any failures or deficiencies in financial fraud risk management that may result in high risks, judicial procedures, regulatory penalties, financial losses, or reputational damage, along with the necessary recommendations to mitigate the risks arising from such situations.

K. Submitting an annual report to the Senior Executive Management, which, in turn, is committed to presenting the report to the Board of Directors or the committee emanating from it that undertakes the tasks of managing financial fraud risks (if applicable). Taking into consideration that this report should, at a minimum, include the following:

1. Results of implementing the Annual Program for Financial Fraud Risks Management, including the outcomes of the tests conducted during the Program's execution period.
2. Summary of a statistical report on financial fraud cases the Company was exposed to, and the deficiencies identified in managing financial fraud risks across all organizational units within the Company, including third parties contracting with the Company.
3. Assessment of the impact levels of fraud risks (financial and non-financial) on the Company.
4. Corrective measures and actions taken, their adequacy, and recommendations specified to address the identified deficiencies, including

disciplinary actions recommended for the Company's employees or measures taken against third parties contracted with the Company.

5. Recommendations related to awareness levels regarding combating financial fraud and managing its risks at the level of the Company's customers or employees, including the adequacy and quality of training programs provided to the Company's employees, and the adequacy of human and financial resources allocated for combating financial fraud cases.

L. Providing the Central Bank, through the Senior Executive Management, with a copy of the aforementioned annual report mentioned in paragraph (K) above, provided that the report should be approved by the Board of Directors or the Regional Manager for foreign company branches.

M. Creating a database (confidential and restricted access with specified permissions) containing all details about actual and suspected financial fraud cases, classified and categorized to facilitate studying these cases and their countermeasures. The information in the database should include, at a minimum, the following:

1. Fraud operation reference number.
2. Fraud operation current status, whether it has concluded, is under investigation and examination, or is active, etc.
3. Relevant information regarding the fraud operation, such as the date of occurrence, duration, names of the fraudsters and involved individuals, the person responsible for following up the case within the Counter-Financial Fraud Unit, and the relevant organizational unit.
4. Estimating the losses resulting from the fraud operation, whether financial or otherwise, as the overall impact of the fraud on the Company's operations or performance.
5. The nature or objective of the fraud operation.
6. The method of committing the fraud operation and its pattern.
7. The procedures conducted to investigate the fraud operation, and the results of the inquiry and investigation.

8. The corrective or disciplinary actions or the judicial prosecutions that have been taken.
9. The measures that have been taken to combat similar cases.

Third: Financial Fraud Risk Management

Financial fraud is considered one of the most dangerous crimes that are ravaging societies, which has grown with technological advancements. This crime relies on the cunning and cleverness of the perpetrator in employing various methods and techniques to deceive victims, making them submit and surrender their funds without the slightest doubt that they are dealing with a fraudster.

Financial fraud can be from inside or outside the financial institution, and it can also be external and involve collaboration or assistance from within, as most of the losses resulting from financial fraud operations may be caused by individuals working within these institutions at all levels of employment. Therefore, financial institutions must consider, while formulating their strategies for managing financial fraud risks that they need to be comprehensive and primarily focus on financial fraud in the workplace with the same importance given to fraud from customers or external sources, including third parties.

The first step in combating financial fraud is recognizing the importance of managing its risks. Therefore, it is imperative for the Company to have a comprehensive strategic plan for protection against financial fraud cases, based on the best practices in this regard. This plan should include the following key elements:

1. Counter-Financial Fraud Policy.
2. Financial Fraud Risk Assessment.
3. Internal Control Systems.
4. Reporting financial fraud cases.
5. Investigating financial fraud.
6. Handling financial fraud cases.
7. Dissemination of awareness and education.

1. Counter-Financial Fraud Policy

To efficiently and effectively manage the financial fraud risks, the Company must establish a comprehensive, written policy approved by its Board of Directors aimed at combating financial fraud. This policy should encompass and manage all measures and procedures applied by the Company across all its organizational units and supervisory and executive levels to protect against both internal and external financial fraud risks.

Furthermore, the primary objective of this Policy is to raise awareness among Company's employees about their roles in combating financial fraud, and clearly defines the person responsible for combating and monitoring financial fraud within the Company, and ensure the implementation of various aspects of the Counter-Fraud Plan. The Policy should also undergo regular review and evaluation, at least annually or as needed, to ensure its effectiveness. In this context, the Company needs to consider the following points:

A. Developing a policy to combat financial fraud, approved by the Board of Directors, and subsequently disseminating this Policy to all employees at all levels of the Company.

B. The Policy should be formulated in collaboration with all organizational units within the Company, as they are better equipped to identify financial fraud opportunities in their respective areas of operation, in a similar manner to involving them in identifying risks associated with their work, whereas teamwork, raising awareness, and promoting a culture of combating financial fraud within the Company can facilitate leveraging collective expertise and ideas.

C. The Policy should be prepared based on the results of the Company's risk assessment, considering both internal and external environment.

D. The policy should include the Company's objectives regarding combating financial fraud, and it should encompass all existing policies and procedures related to the combating and monitoring of financial fraud.

E. The Senior Executive Management should adopt and implement initiatives that demonstrate their commitment to acting with integrity and adhering to the principles and guidelines of the Counter-Financial Fraud Policy. They should be aware of their responsibility and accountability for fostering an ethical climate to deter any fraudulent attempts and encourage reporting of any violations of accepted standards.

F. Ensuring an adequate supply of human, financial, and technological resources to guarantee the success of the Counter-Financial Fraud Policy. This will send a clear and explicit signal to the Company's employees that the Senior Executive Management will not tolerate any leniency in tackling financial fraud.

G. A clear message should be conveyed to all employees within the Company regarding the importance of combating financial fraud, in order for them to understand their responsibilities in adhering to the Counter-Financial Fraud Policy and actively participating in detecting and reporting any suspected cases of financial fraud while also cooperating with investigations as per their respective responsibilities.

H. The Policy should be subject to periodic review, and whenever deemed necessary, to reflect changes in the Company's operational environment and services, and to assess its capability in meeting the reevaluated objectives. This is to maintain the efficiency and effectiveness of this policy in combating financial fraud.

When preparing the Counter-Financial Fraud Policy, the Company should consider including relevant work procedures related to combating financial fraud, in which, clear steps shall be defined for the necessary procedures to be taken in response to reported or suspected cases of financial fraud, as well as measures to prevent or reduce financial fraud cases, in a manner that covers all types of fraud the Company has been or might be exposed to in the future, taking into account its continuous updating based on the latest developments, so that employees and relevant third parties can view and apply it based on their respective positions.

Many companies adopt Counter-Financial Fraud Policy to demonstrate their commitment to combating financial fraud and addressing it within any Company's policies or as a separate policy. The Counter-Financial Fraud Policy aims to protect the Company by enhancing financial fraud risk management and defining clear steps to be taken regarding reported or suspected fraud cases, in addition to measures that will be taken to limit or reduce financial fraud risks. Accordingly, the policy should include the following key components as a minimum:

A. Roles and responsibilities of the Board of Directors and Senior Executive Management.

B. Roles and responsibilities of the Counter-Financial Fraud Committee (if any).

C. Roles, responsibilities and powers of the Counter-Financial Fraud Unit or the organizational unit concerned with carrying out the financial fraud prevention tasks.

D. Roles and responsibilities of other organizational units within the Company towards combating financial fraud.

E. Principles ensuring the Counter-Financial Fraud Unit's right to investigate financial fraud cases and to report and disclose investigation results to Senior Executive Management and, if necessary, to the Board of Directors, as well as the procedures applied before/during the investigation process of financial fraud cases.

F. Procedures and controls required for monitoring, detecting, and preventing financial fraud cases.

G. Mechanisms, procedures, and communication channels for reporting suspected cases of internal fraud and the responsible for investigating internal fraud within the Company, identifying channels and mechanisms for receiving reports on external fraud cases and ensuring the available protection for fraud whistleblower.

H. Principles for reporting financial fraud risks to the Senior Executive Management and the Central Bank.

I. The mechanisms for reporting, and exchanging information and data with the Central Bank, other relevant competent authorities, and the Anti-Money Laundering and Counter-Terrorist Financing Unit, and in accordance with the provisions of legislation in force.

J. Principles and mechanisms for record-keeping and preserving documents and evidences related to financial fraud cases in accordance with the legislation in force.

K. Roles, responsibilities, and powers of frontline customer-service employees in handling reports received regarding financial fraud operations.

L. Principles that ensure the dissemination and promotion of awareness and culture towards methods of combating financial fraud and managing its risks for the Company's customers or employees, including accountability in case of negligence or misconduct.

M. The principles of supporting and promoting the values of honesty, integrity and uprightness to thwart any fraud attempt and encourage reporting any breach of accepted standards.

2. Financial fraud risk assessment

Financial fraud represents one of the risks that the Company might face and it must ensure its assessment as part of the overall risk assessment process periodically conducted, in order to ensure that the Senior Executive Management and the Board of Directors have a comprehensive understanding of all the necessary information for combating financial fraud effectively.

The review should encompass all Company's functions, processes, and systems, addressing both internal and external fraud risks. It should identify the Company's exposure level and the nature of vulnerability to this risk, enabling the determination of countermeasures, because the review process is considered the mean capable of identifying and evaluating inherent risks. As well as specifying the measures that have been taken and those needed to be taken to reduce and mitigate the severity of risk levels.

When implementing control measures, it is essential to consider that sources of financial fraud can be from within or outside the Company. Additionally, collusion from within can undermine the effectiveness of certain control measures, such as segregation of duties, for example.

The process of assessing financial fraud risks is carried out similarly to any other risk assessment process, comprising three main components that can be taken into account when implementing a financial fraud risk assessment program. These components are as follows:

A. **Identifying Inherent Fraud Risks:** At this stage, the available information about fraudulent activities and electronic threats that the Company or its customers may be exposed to is gathered. This process includes considering all types of fraud schemes that may occur, regardless of the incentives, pressures, or opportunities causing the fraud, including security vulnerabilities that could lead to electronic fraud activities.

B. **Evaluating the risks' likelihood and impact:** This stage involves assessing the relative probability of occurrence for each threat/fraud scheme and the potential impact of the risks associated with fraudulent activities based on the available data.

C. **Responding to fraud risks and calculating residual risks:** In this stage, residual risks are calculated after implementing all types of control measures, and determining the most suitable response to address the risks based on clear criteria, such as cost-benefit analysis, and identifying the specific controls that need to be implemented.

To assess financial fraud risks, it is essential to first identify these risks in order to develop a comprehensive understanding of the financial fraud landscape within the Company. This can be achieved by identifying both internal and external data sources to detect and monitor emerging fraud threats that the Company or its customers may face. The following methods can be employed by the Company to recognize and pinpoint fraud risks.

A. Brainstorming sessions and recurring meetings conducted to identify potential fraud scenarios.
B. Internal or external audit reports and the outcomes of investigations of financial fraud cases, along with the analysis of fraud scenarios encompassing attempted and successful fraud incidents, to identify common methods, techniques, and procedures used in fraudulent activities.
C. New and emerging fraud patterns identified by fraud detection systems, fraud investigators, or the Counter-Financial Fraud Unit within the Company.
D. Databases containing fraud scenarios available from the Compliance Monitoring Unit, the Cybersecurity Unit, and the Incident Management Team within the Company, as well as from the Cybersecurity Incident Response Team, or the disseminated bulletins from the Central Bank and other relevant competent authorities, following guidelines issued by the International Criminal Police Organization (INTERPOL).
E. Reliable and relevant external sources regarding local and global fraud trends.
F. Available and common fraud scenarios across online platforms related to the electronic payment sector.
G. Monitoring the latest trends in fraud scenarios and electronic hacking attempts.

Financial Fraud and Cybersecurity:

The Company should ensure alignment between the operational capabilities of the Counter-Financial Fraud Unit and its Cybersecurity Unit, at a minimum, by:

- Defining clear roles and responsibilities between both units.
- Implementing cross-training between the two units.
- Establishing multi-disciplinary contacts between both units to exchange knowledge regularly.
- Developing joint task forces between both units to align working practice and promoting collaborative work.
- Undertaking joint threat assessment workshops or fraud scenario analysis with other business units to collectively identify threats and share insights, and storing relevant threat information in a centralized repository, with access restricted to relevant stakeholders.

- Identifying opportunities to unify fraud and cyber prevention and detection systems and tools (e.g., provision of data on user monitoring or customer location through IP address).
- Coordinating corrective actions for fraud cases (e.g., taking down fake websites set up to capture customer details).
- Conducting joint retrospective lessons-learned exercises following fraud incidents that relate to data, systems, processes and controls.

By definition, fraud involves intentional misconduct designed to evade detection, therefore, the Fraud Risk Assessment team must be involved in the strategic thinking to anticipate fraud scenarios that the Company may face. Strategic thinking, which is crucial in designing fraud detection measures that perpetrators may not anticipate, requires a skeptical mindset that relies on asking probing questions leading to the design of detection procedures. Examples of such questions include:

A. How can the fraudster exploit vulnerabilities in the Company's work environment and implemented controls?

B. How can the fraudster bypass the applied control measures in the Company?

C. What can the fraud perpetrator do to conceal the fraudulent activity?

Afterward, the Company proceeds to identify and manage financial fraud risks that the Company or its clients may exposed to by conducting comprehensive assessments of financial fraud risks at the organizational level, to identify and evaluate fraud risks, and the potential events that may be exposed to, and their likelihood and impact. Additionally, developing plans and recommendations to mitigate the remaining risks as much as possible, covering all functions, operational units, and technological systems within the Company. It is essential for the Financial Fraud Risk Assessment process to be based on a documented methodology that considers the following factors:

A. Identifying potential types of fraud that the Company or its clients may be susceptible to by gathering relevant information about internal and external

threats that could target the Company's services and electronic channels, including its employees and technological systems.

B. Evaluating the likelihood of potential fraud risks occurring and their potential impact on the Company and its clients If they occur, considering the following factors during the assessment of potential fraud risks:

1. Potential fraud risks, whether internal (that can be committed by or with the assistance of employees within the Company) or external (that can be committed by individuals outside the Company).
2. Risks associated with the services and products offered by the Company and how they could be exploited for committing fraudulent activities.
3. Customer risks, including, for example, the type of customer, the number of customers, and the level of fraud awareness among customers.
4. Electronic delivery channel risk that customers can use to contact the Company or access services and products.
5. Jurisdiction risks, including risks related to the use of services and products provided by the Company that can be accessed in foreign countries or high-risk regions.
6. Transaction risks, such as the methods of conducting transactions, receiving funds, or transferring value, and so forth.
7. Third party risks, whether they are agents providing the Company's services and products, establishing a business relationship on behalf of the Company, or offering technical and technological services related to the Company's operations.
8. Risks associated with the Company's technological systems, including access control lists, business execution plans, and other related aspects.

C. Conducting the Financial Fraud Risk Assessment at a minimum on an annual basis, and updating it as needed based on the variables that may arise in the fraud risk environment, whether internal or external. These variables may

include, but are not limited to, deficiencies or weaknesses identified in the control environment, new regulatory requirements issued by the Central Bank, new products, services, operations, or technologies, new marketing channels for services and products, changes in the Company's internal environment such as organizational structure, job changes, or employee turnover, and new relevant information acquired or received by the Company regarding fraud. Consequently, updating and reviewing the fraud risk file regularly.

D. Ensuring the effectiveness of the implemented controls to detect and prevent potential financial fraud risks, including examining internal vulnerabilities within the Company that may increase opportunities for financial fraud, and reviewing analytical data related to financial fraud operations as both a preventive and investigative tool to detect fraudulent activities.

E. Identifying residual fraud risks that the Company may still be exposed to after ensuring the effectiveness of the implemented controls.

F. Developing action plans to address the residual fraud risks that fall outside the acceptable risk tolerance or could lead to a breach of the Company's systems and its ability to respond to and continuously monitor these risks to ensure they remain within the Company's desired risk level. At a minimum, these plans should encompass the following:

1. Designing tools and control measures to monitor and combat the residual fraud risks and mitigate them in the event of fraud occurrences or timely detection failures. Additionally, assessing the effectiveness and efficiency of these control measures, monitoring them, and continuously updating them.

2. Developing and monitoring early warning indicators and key financial fraud risk indicators, applying them across all units in the Company, and regularly monitoring and analyzing the results, issuing periodic reports to make timely and appropriate decisions, mitigating risks, and minimizing losses as much as possible, whether those indicators are related to employees in particular, the information technology and communication environment, associated procedures and policies, third parties, or Company customers.

3. Establishing a reporting and handling mechanism for financial fraud cases when they are detected or suspected.

G. Proposing the necessary procedures, measures, plans, and controls to combat financial fraud cases within a specified timeline.
H. Implementing a specific approach to investigate financial fraud operations and corrective actions to address fraud appropriately and in a timely manner.
I. Following up on the implementation of corrective and preventive actions to combat financial fraud in the Company against the identified risks during the review process.
J. Documenting the review process in a manner that allows for easy reference and retrieval.
K. Developing a Financial Fraud Monitoring Plan using the warning indicators identified by the Company.

3. Internal Control Procedures

Internal control procedures are among the most critical elements in combating financial fraud. Regulatory frameworks issued by the Central Bank obliges companies to establish internal control systems to meet corporate governance requirements. The same applies to combating financial fraud, as the Central Bank still emphasizes that financial fraud is a risk like other risks that the Company is exposed to. Therefore, management should establish internal control measures that effectively address this risk.

In this context, the Company should establish documented internal control systems within a written policy and define clear and comprehensive procedures to reduce and combat the risk of financial fraud. The Company must ensure the integration of these controls with the procedures and controls governing its activities, services, employees, customers, and third parties, and it is possible to automate these controls to a significant extent, based on the Company's capabilities and resources. These controls are implemented to support the company's overall objective, which is to minimize occurrences of financial fraud to which the Company, its contracted

third parties, or its customers may be exposed to. These controls can be categorized as follows:

A. **Preventive controls;** include the measures taken before fraud occurs, some of which are linked to the organizational structure. As segregation of duties - meaning not allowing one person to have control over all aspects of transaction processing - serves as a preventive control. Other preventive controls can be incorporated into the Company's systems, such as security and technical controls specified in the Instructions of Cyber Risks Resilience, like password policies, and access controls that prevent unauthorized access to systems or data, that can thwart fraudulent activities before they happen. Generally, preventive controls are considered the most effective, efficient, and cost-effective controls.

B. **Detective controls;** these controls are used to identify violations if they exist. They are also designed to provide a certain level of assurance that preventive controls are functioning as intended. Implementing monitoring controls and indicators on the Company's financial transaction monitoring systems, and relying on detection technologies like Intrusion Detection Systems (IDS) are examples of detective controls. Detective controls are generally more costly and time-consuming than preventive controls. However, the significance of detective controls in mitigating financial fraud risks should not be underestimated.

C. **Corrective controls;** these are used to address financial fraud cases, violations, or activities related to threats after their detection or following the occurrence of a fraudulent incident. Corrective controls can help improve preventive and detective controls, thereby enhancing the Company's ability to respond in subsequent instances.

Preventive controls:

In order for the Company to effectively combat financial fraud by relying on its controls within its internal control environment, its responsibility to establish and activate specific controls and procedures designed to counter financial fraud, which

are documented in the Counter-Financial Fraud Policy to prevent the risks associated with financial fraud. The key preventive controls include the following:

A. Ensuring the integration of the controls specified for combating financial fraud with the controls imposed on the Company's operational environment, which govern all Company's functions, services, channels, facilities, and customers.

B. Implementing Controls that govern restricted and monitored access to risky areas, limiting and restricting privileges at all administrative and executive levels within the Company, including its electronic channels, based on the risky areas associated with geographic location, customer, electronic channel, and the offered services and products.

C. Conduct Strong customer authentication to authenticate the customer's identity using at least two factors and avoid relying solely on One Time Passwords (OTPs) sent via SMS, but instead implementing additional factors, based on their degree of risk, in the following cases, among others:

1. When establishing a business relationship.
2. Using/ Accessing Electronic Channels, whether through mobile applications, websites, or others.
3. Performing financial or non-financial transactions, taking into consideration the type of transaction and its level of risk.
4. Approval of transactions through Mobile App (e.g., sending a push notification to the mobile app on a known and trusted device).
5. Geolocation (e.g., verifying location using GPS, IP address or checking mobile network).
6. Customer behavioral profile (e.g., variations to usual transaction volume, value, frequency and/or currency).
7. Utilizing human body's biometric characteristics (e.g., fingerprint, facial recognition, or iris scan).

8. Biometric behavioral profile (e.g., identification of changes in the way a customer or employee uses a browser or device).
9. Change of electronic channel sensitive settings, such as changing the password, username, or other sensitive data.
10. Adding a payment card to an electronic wallet or on a website or other platforms.
11. Resetting security credentials to access electronic channels or using payment instruments following failed attempts to access or use them.
12. Activating the mobile application on a new device.
13. Logging into digital products from a previously unknown device or location.
14. Change of account holder details (e.g., address or contact details).
15. Change of language used on the account (e.g., Arabic to English).
16. Resetting the password or PIN.
17. Issuance and activation of a new payment card.
18. Reactivation of inactive accounts, which refers to those accounts that have not been logged into by the customers within a specific period defined by the Company before they become dormant accounts according to the provisions of the applicable regulations.

D. Company should require a third authentication factor (e.g., conducting a call to a known number associated with the customer's account, or sending a one-time password (OTP)) in any of the following cases:

1. A user log-in attempt to electronic channels is detected as an anomalous session (e.g., a device ID or location is different from previously known log-in parameters or the IP address is flagged as a risk).
2. A transaction is instructed from a non-trusted device to a newly added beneficiary.

3. Executing behavior or a set of activities that may indicate fraud or unauthorized account access according to specific predefined scenarios.
4. Exceeding the normal rate of payment or transfers (e.g., executing five payment or transfer transactions for a customer per hour), considering that the Company may restrict account activity until customer identity is authenticated and the reliability of the customer's device is verified.

E. Ensuring that individuals responsible for implementing the control measures to combat fraud are sufficiently independent from those who oversee their performance. This includes establishing appropriate controls to deter and avoid conflicts of interest and related party transactions for their directors, managers, employees, external businesses, and contractors, including but not limited to:

1. Creating a policy that clearly outlines prohibited behaviors.
2. Limiting the flow of information between internal departments and employees through information barriers.
3. Providing guidance, instructions and examples on avoiding conflicts of interest.
4. Requiring immediate disclosure of any conflicts or potential conflicts.

F. Company's fraud prevention standards should include controls designed to prevent internal fraud, including:

1. Including the employment policy with procedures that ensure the integrity of prospective employees before their appointment, and establishing adequate procedures to monitor employee's behavior and implement indicators that indicate any misconduct or lack of integrity. These indicators may include unjustified enrichment, hesitation in taking leaves, sudden refusal of promotions, or unexpected resignations without valid justifications.
2. Specific controls and procedures to combat internal financial fraud cases by employees may include mandatory vacations, unexpected rotation of employee programs and tasks, auditing employee accounts during their leaves, establishing controls governing work performed by relatives or related

parties, and implementing policies for accepting gifts to detect any potential bribery cases that may arise.

3. Safeguarding, maintaining, and securing valuable assets, sensitive systems, and confidential data within the Company.
4. Strictly applying the principle of segregation of jobs and duties in all Company operations, including separating control responsibilities from control implementation tasks, as well as segregating control of asset from the control of documents related to these assets.
5. Requiring employees to adhere to the Code of Conduct
6. Segregation of duties in payment and fulfilment processes supported by documented authorization matrices.
7. Dual controls or secondary checking of control operation, with an additional review or approval process for transactions above thresholds defined by the Company (e.g., value of transaction or payments to a new supplier) or higher risk transactions (e.g., access to dormant accounts).
8. Restricting access to customer's confidential details for all employees (e.g., online credentials, OTP messages).
9. Restricting access to confidential customer account data (e.g., account balance) where visibility is not required in the job role (e.g., IT employees). Where access is required, activities should be logged and securely stored. Defining requirements for appropriate handling of confidential data, access controls to such data, based on related defined and approved authorization matrices.
10. Controls to safeguard the physical security of assets (e.g., requiring staff identification at all times, securing and tracking equipment and restricting access to sensitive assets).

G. Company's fraud prevention standards should include controls designed to prevent external fraud, including:

1. Hotline available 24 hours to report suspected fraud and take immediate action to respond to the fraud (e.g., blocking account access or payment instrument).
2. The provision of an emergency stop self-service capability for customers to immediately block their payment instrument or freeze their account and block further transactions if they suspect their account or payment instrument has been compromised.
3. Customer identity and access management controls for online/mobile accounts and digital products.
4. Use of blacklists to screen and block suspicious IP addresses, e-mail addresses, and compromised devices or those that have previously been used for fraud (e.g., mobile phone number registered to an account which has been used to conduct fraud).
5. Requiring users of electronic channels to consent to the activation of GPS during an active session to allow the Company to monitor their locations.
6. The capability of mobile apps to detect devices which are subjected to jailbreaking or rooting, and subsequently block the use of the app or restrict access to sensitive data or features.
7. A restriction on concurrent log-ins to customer's account or a limitation on the number of devices through which a customers can access their account.
8. Creating profiles for user behavior patterns, which provide the ability to detect any unusual behavior, including monitoring inactive services, products, or accounts and implementing necessary controls when they are used; to enhance customer identity authentication.
9. Sending notifications to the customer when changes are made to his/her account data, using Short Message Service (SMS) on their registered mobile number, or through email, or both.
10. Setting a default limit for single, daily, and monthly transactions, which should be periodically reviewed and updated where required (e.g., review of

customer profiles and behaviors, and actual fraud cases) with the option for the customer to set those default limit by himself.

11. Implementing additional verification checks to authenticate the customer's identity in any of the following cases, where the verification checks include (automated call-backs, manual call-backs, or sending a text message to the registered mobile number, and authentication via biometrics on registered mobile recognized by the Company).
    a. Unusual transactions (e.g., transactions after a period of account dormancy, changes to customer behaviors).
    b. Unusual patterns of transactions (e.g., multiple payments to the same beneficiary in a short period).
    c. Transactions exceeding a defined value threshold.
    d. Requests to increase the single or daily transaction limit.
    e. Initial transactions after registration for electronic channels, or registration of a new device.
    f. Transactions occurring in a high-risk location (e.g., using mobile device geolocation data to require verification if a user attempts to access products and services while in a foreign country which is not in line with user behavior profile).
12. Periodic inspection of electronic channels for evidence of suspicious activity or devices that could compromise card security.

Detective controls:

In order for the Company to effectively combat financial fraud within its internal control environment, it is responsible for adopting and implementing detection standards for financial fraud cases that it may encounter, aligning with the fraud risks that affect the Company and its customers. To achieve this, the Company should consider the following:

A. Define, approve, implement and maintain fraud detection standards in a manner that enables the Company to effectively combat both internal and external fraud risks affecting the Company.

B. Review and update fraud detection standards on a periodic basis and in response to material changes to the fraud landscape or the Company's Fraud Risk Assessment.

C. The compliance with fraud detection standards should be monitored.

D. The effectiveness of fraud detection standards and related controls should be measured and periodically evaluated.

E. The output of the Fraud Risk Assessment should be used to determine where detection activity is focused, and controls should be proportionate to the risk appetite of the Company.

F. Where the inherent risk of fraud is assessed as higher, the fraud detection standards should require additional detection controls (e.g., real time monitoring, additional data sources or Machine Learning models) or more stringent detection threshold criteria (e.g., lower monetary limits before an alert is raised).

G. Fraud detection standards should include at a minimum:

1. Data sources used to inform the detection of suspicious activity and fraud (e.g., customer records, transactional/payment systems, identity and access management, external databases).

2. The controls implemented to detect suspected fraudulent activity (e.g., escalation of high-risk events and transactions, secondary checking, reconciliations, exception reporting, internal training).

3. The controls implemented to detect suspected fraudulent activity relating to the nature of financial transactions conducted by the Company's customers, whether outgoing or ingoing.

4. Systems and technology implemented to detect potential fraud (e.g., fraud detection software, alerts on high-value events or transactions, access monitoring).

5. Roles and responsibilities for fraud detection (e.g., system calibration, reviewing manual fraud referrals, alert triaging and management, escalation point for potentially significant incidents, supervision and oversight).

6. Rationale outlining why the detection systems and controls are appropriate to the risks faced by the Company.

H. Company should consider the following requirements when documenting the people, process, and technology requirements for fraud detection:

1. Employee activity data (e.g., system access, invoices and payments, approvals).
2. Customer account activity (e.g., transactions, payments).
3. Customer account access and management (e.g., log-in geolocation, device usage, changes to static data).
4. Third party activity data (e.g., access to and use of Company's systems or data, instructions on behalf of customers, referrals from agents).

I. Company should have adequate resources in place to manage the outputs from manual and automated fraud detection (e.g., sufficient employees to process alerts, appropriate skills and training for employees to complete investigations, and a workflow system to allocate alerts).

J. Implementing and maintaining fraud detection systems to identify anomalies in transactional data, and customer or employee behavior, while incorporating necessary indicators and scenarios, taken into consideration the following points:

1. The scope of fraud detection systems includes monitoring customer products and services, as well as internal systems of transactions or behaviors that may be indicative of fraud.

2. Fraud detection systems should operate 24/7 with appropriate resources in place to manage outputs on a timely basis.
3. Developing holistic sources of data to be used to inform detection of suspicious activity and fraud.
4. Calibrate and test detection scenarios to validate they are working as designed and enabling monitoring in accordance with the company's risk appetite.
5. Implementing feedback loops to monitor and enhance the performance of systems and effectiveness of scenarios and parameters by reviewing fake alerts.
6. Periodically review scenarios and parameters to ensure they remain appropriate in view of the outcome of the Fraud Risk Assessment. Moreover, to target proactive prevention and detection of new or emerging patterns identified through continuous monitoring or incoming notifications.
7. Periodically test the effectiveness of systems through ongoing tuning and calibration measures such as data mapping and input validation, model validation, scenario effectiveness testing and reporting.
8. Update user behavior patterns and rules to account for the latest threats and fraud typologies.
9. Retain a documented record of changes made to configuration or rules and the rationale for the decision.
10. Monitor for unauthorized changes to the system (e.g., rule tampering or disabling of monitoring).
11. Awareness of the system's operating rules, including fraud detection rules and scenarios, should be limited to a specific group of employees specialized in combating financial fraud. This should not include employees or third parties responsible for the operation of processes and controlled procedures.

K. Design and implement controls to monitor customer products and services for behaviors that may be indicative of external fraud. At a minimum these should address the risk presented by:

1. First party fraud – Where a customer of the Company misrepresents their identity or gives false information to commit fraud using their own account, payment instrument or other product.
2. Second party fraud – Where a customer or individual knowingly provides their personal information or allows their identity to be used to commit fraud.
3. Third party fraud – Where an individual obtains a customer's details without his consent or knowledge, then uses the information to commit fraud.

L. Design and implement controls to monitor employees in roles identified in the Fraud Risk Assessment as presenting a risk of internal fraud, including but not limited to:

1. Audit trail of employee access to the Company's core systems.
2. Systematic log of staff activities for all customer and financial accounting systems and databases (e.g., recording an audit trail of an employee making changes to a customer address, adding a payee, instructing a payment, authorizing a withdrawal, increasing transaction limit).
3. Monitoring for unusual behaviors or activities (e.g., transactions outside working hours, process exceptions or overrides completed without appropriate approvals).
4. Ensuring the reconciliation and settlement process between the financial systems and other operational systems within the Company, in addition to organizing and reviewing bank accounts. Also, verifying the re-balancing of all temporary accounts in the Company (intermediate accounts).
5. Monitoring and appropriate approval of the use of documentary documents or instruments through which claims are paid or Company receivables are collected.

6. Monitoring of employee complaints and anonymous reporting lines.

Corrective Controls:

In order for the Company to effectively address financial fraud cases relying on its internal control environment, it is responsible for adopting and implementing corrective measures to address financial fraud instances, violations, or related threatening activities after their detection or occurrence. Corrective controls may help improve preventive and detective controls, thus enhancing the Company's ability to respond in subsequent instances. To achieve this, the Company needs to consider the following:

A. Define, and implement an approved Fraud Response Plan, reviewing it as needed, and where appropriate aligned with the enterprise incident management process.

B. The compliance with the Fraud Response Plan should be monitored.

C. The effectiveness of the Fraud Response Plan and related controls should be measured and periodically evaluated.

D. The Fraud Response Plan should require prompt and competent assessment, investigation, and resolution of all suspected or identified fraud cases.

E. The Fraud Response Plan should include at a minimum:

1. Methods through which the Company is alerted to suspected or identified fraud, including reporting channels available to customers, employees and third parties.

2. Roles and responsibilities for individuals and teams required to respond to a potential fraud.

3. Decision-making authority and referral procedures for escalations within and outside the Company including taking legal actions and referring matters to relevant competent authorities (e.g., referral to specialists for complex cases, Senior Management for potentially material frauds, external counsel if there are legal concerns).

4. Procedures to quickly respond to potential fraud cases identified by the Company, informed by the customer, other companies, the Central Bank, other competent authorities, or any other third parties. Bearing in mind that this includes precautionary measures to seize the funds received in accordance with the rules and regulations in force.

F. The actions the Company will take when fraud is suspected or has been identified, including but not limited to:

1. Coordinating appropriate resources to manage alert and case volumes.
2. Recording and performing an initial assessment of all alerts or formally submitted reports of fraud.
3. Where an alert or referral is assessed as not requiring further investigation, a rationale must be documented that explaining the decision.
4. Investigating all instances where it is suspected fraud may have been committed or has been identified.
5. Mechanisms for extracting, retaining, handling, and copying evidence, as well as the mechanism for delivering it to investigative or judicial authorities. Moreover, mechanisms must be established in a way that ensures data integrity and confidentiality.
6. Keeping a comprehensive record of all evidence and investigations of potential and actual fraud for a period not less than the period defined in the Anti-Money Laundering and Counter-Terrorism Financing legislation, and in line with the periods prescribed in relevant regulations in force.

G. The process to be followed in the event a potential fraud incident is detected outside of the normal working hours of the Company.

H. When an actual or potential fraud relates to services and product offered to a customer or a payment to/from the Company, the Fraud Response Plan should require to:

1. Identify if a potentially fraudulent transaction has been completed or is in the process of being completed.
2. If a transaction has not been completed; take immediate action to block or hold the transaction and proactively coordinate with any corresponding other parties.
3. Proactively respond to requests relating to suspected fraudulent transactions when receiving a notification from a customer, another Company, competent authorities, or the Central Bank.
4. Block or freeze the account or any payment instrument linked to it, to prevent further transactions until the investigation is complete, and where necessary security credentials are reset or a new card is issued, or anew account is opened and so forth.
5. Block any further transactions to or from any accounts outside the Company that were used to perpetrate the fraud operation.
6. Cooperate with other companies when needed if a request for freezing a product is received and there are justifications for suspicion based on the Central Bank's orders issued in this regard.
7. Contact the customer or third party to communicate actions taken, and the necessary steps to mitigate the consequences of the fraud as much as possible.
8. Verify the identity of the customer before reactivating his account and the related payment instruments that have been frozen due to exposure to fraud.

I. It is beneficial for the Company to implement a Fraud Case Management system to enable efficient and effective response to fraud cases, by establishing a database for fraud cases. Such systems facilitate the documentation and recording of all relevant data, information, and alerts related to suspected or actual fraud cases, monitoring, investigating, and resolving such cases, along with generating internal and external reports concerning fraud incidents. Taking into consideration that this system should have the capability to:

1. Restrict user access to authorized individuals and roles.
2. Create a workflow aligned to the operating model of the company based on defined authorization matrices in this regards.
3. Be configurable to adapt to changes in the Company's operating model or Fraud Response Plan.
4. Categorize fraud cases based on the units or departments they are associated with.
5. Categorize suspicions of fraud to define reporting lines.
6. Track the fraud case throughout its entire lifecycle, starting from the initial alert to its resolution, along with all relevant data related to the fraud process (e.g., the serial number, date of the initial alert or notification, date and time of the fraud incident, customer name, account number, payment instrument number, the method/channel used in the fraud, parties involved, fraudster's information, the value of the fraud, methods and patterns used, and other pertinent details).
7. Record investigative steps followed.
8. Act as a repository for all information required to investigate and resolve the fraud case (e.g., related party information, case notes, documentary evidence, customer communication, rationale for decision).
9. The results of resolving the fraud case, including any incurred losses and imposed corrective actions.
10. Retain records for the periods specified in the Company's policy and in accordance with regulations in force.

J. The lessons learned should be incorporated into the plan, including follow-up actions to address fraud cases. This includes implementing control measures to reduce the recurrence of such cases and verifying the update of risk records in case these risks were not initially included in the risk register.

The Company must ensure the presence of an independent, continuous, and reliable Follow-up process to protect it from the risks of financial fraud to the maximum extent possible. The Follow-up process is categorized into two types as follows:

A. **Internal Follow-up;** It involves monitoring the Company's internal controls through periodic review reports that are submitted to the Board of Directors, whether from the Internal Audit Function or any reports submitted by the Executive Management related to fraud operations within the Company. Key processes often associated with fraud operations and subject to review include ensuring no manipulation in the Company's accounts, verifying the existence and activation of various security controls for access to the Company's assets (Physical access) or to its systems and data. Additionally, the presence and activation of appropriate awareness programs for employees, customers, or third parties dealing with the Company, as required.

Financial Fraud and Internal Audit

Counter-Financial Fraud Function is closely related to the Internal Audit Function, and it is essential for the Company's Internal Audit Unit to conduct audits to verify that the tasks associated with the Counter-Financial Fraud Function have been appropriately and effectively executed. To achieve this proper linkage between the two functions, the following considerations are required:

- Ensuring that Counter-Fraud audits are performed independently and according to generally accepted auditing standards and the Central Bank's relevant regulation.
- Defining the frequency of Counter-Fraud audit according to risk-based approach, based on the outputs of the Fraud Risk Assessment. This involves developing an approved audit plan that addresses the Company's components, including personnel, processes, and technological systems.

- The Internal Audit function should complete periodic validation of the implementation of Counter-Financial Fraud related corrective actions, including those resulting from the Central Bank's instruction.
- Ensuring that the Counter-Fraud auditors have the requisite level of competencies and skills to effectively assess and evaluate the adequacy of procedures, processes and controls implemented, in accordance with the Counter-Fraud Policy.
- Including in the audit reports the findings and recommendations related to the audit processes on financial fraud prevention efforts, while considering the follow-up on the observations generated by the audit process and monitoring their implementation levels.

B. **External Follow-up;** here, the Company relies on an external entity to assess the effectiveness of internal operational controls. The Central Bank ensures the evaluation of the Company's internal control systems as part of its supervision and oversight process for companies. To ensure the effectiveness of external Follow-up processes, it should not be limited to auditing accounting controls and financial information accuracy. Instead, it should encompass a review of internal operational controls, the adequacy of administrative systems, and security measures. Although the external audit process does not provide sufficient effectiveness in detecting and combating financial fraud, it does offer a certain level of control by reducing the risk of financial fraud resulting from negligence in complying with internal control measures.

4. Reporting Financial Fraud

The Company must consider providing clear and appropriate reporting mechanisms that ensure sufficient coordination regarding matters related to combating financial fraud with relevant stakeholders to the Company, both internal and external, including the Central Bank, other competent authorities, and the Anti-Money Laundering and Counter-Terrorism Financing Unit. These mechanisms should include the following:

A. The reporting process regarding incidents of financial fraud should be directly linked to the head of the Financial Fraud Unit or his representative, or any individual delegated to carry out the responsibilities of combating financial fraud, such as the Compliance Officer.

B. The relevant units/persons involved in the event must be immediately informed, whether they are within or outside the Company, through the provision of dedicated reporting channels, such as email, formal letters, electronic systems, and others.

C. Upon confirming a financial fraud, the Company must activate appropriate escalation procedures to investigate the fraud case. This includes notifying other financial institutions that have been affected or suspected to be involved in the fraud case, working jointly to resolve the fraud case according to the central bank's guidelines. If necessary, the relevant competent authorities (law enforcement agencies) should be informed, based on the specifics of the fraud case. The Central Bank should also be notified, along with the Anti-Money Laundering and Counter-Terrorism Financing Unit. It is important to note that reporting the fraud does not absolve the Company from its responsibility to refer the fraud case to other relevant security authorities. Additionally, reporting the fraud does not diminish the Company's responsibility to address the fraud and bear its consequences.

D. Board of Directors, Senior Executive Management, and the Internal Audit department must be directly notified when fraud occurs. This includes promptly reporting fraud cases that have a significant and direct negative impact on the Company's current or future operations after the event has been discovered, encompassing all relevant details, in addition to regular reports provided to them.

E. Establishing comprehensive training programs to clearly educate employees on the reporting system's structure and the procedures for handling reports related to fraudulent activities, and the preventive measures to protect whistleblowers who report suspicious activities. It is essential for the Company to ensure that employees understand the importance of reporting all fraudulent

attempts, including failed ones, as unsuccessful attempts of fraud are just as serious as successful ones. If these unsuccessful attempts go unreported, it provides fraudsters with the opportunity to learn from their mistakes and potentially try again in the future.

F. Raising customer awareness regarding fraud methods and the mechanisms for reporting any suspicions of fraud or instances where they have been victims of fraud, the timing and the importance of reporting as quickly as possible without delay, the level of responsibility they bear if they delay or fail to report, and the potential financial losses they may incur as a result.

G. As part of the fraud reporting system, the Company should develop appropriate mechanisms and policies to support and protect whistleblowers from retaliation resulting from reporting fraudulent activities, such as setting of alarm bells policy, and this should not cover malicious or ill-intentioned reports, and appropriate measures should be taken to alleviate any fears among employees about reporting suspected fraud.

5. Fraud Investigating

After receiving a report of fraud or detecting fraudulent activity, the Company is required to initiate an investigation into the fraud case. The Company's investigation team needs to work collaboratively with all relevant parties while adhering to security and confidentiality controls to ensure that the incident does not negatively affect the Company's reputation and business continuity, and to maintain the fraudster's belief that he has not been detected yet. To achieve this, the Company should undertake the following steps:

A. Ensure the presence of clear and formal procedures for conducting investigations, and training employees accordingly. In this regard, the Company should, at a minimum, guarantee the following:

1. Maintaining records of all known cases of fraud discovered and investigations conducted, and developing systems to follow up investigations and report their status and results of its progress and updating them appropriately.

2. Defining the responsibilities of the person who receives a notification of suspected or discovered fraud clearly in the Company's guidelines and policy for combating fraud. These responsibilities include recording all the details of the notification or suspicion as soon as possible in a confidential file referred to as a case report. These details include, at minimum, the following:
    - Date and time of the notification, incident or suspicion.
    - Name of the complaint/ the notifier.
    - Details of the communications and the reporting channel used.
    - Nature of the notification.
    - Time or period of alleged fraud.
    - Circumstances of the alleged crime.
    - Perpetrator of the fraud if detected.
    - Value of the fraud, and the instrument or channel through which the fraud was committed.
    - Any written notification or supporting documents submitted in the reporting process (must be stamped and documented).

B. Typically, there are several pieces of evidence that the Company can rely on when making decisions during the investigation of the fraud incident, including:

1. Geolocation Data: Identifying the geographic location of the transaction's completion and ensuring its compatibility with the customer's residence or workplace location.
2. Transaction Timing: Was the timing of the transaction reasonable for the customer or consistent with other evidence, such as the geolocation data.
3. Customer IP Address: Does the buyer's IP address match the customer's address? If not, this may indicate a fraudulent transaction.

4. Protection services offered by global companies (3D Secure), such as (Verified by Visa) or (MasterCard Secure Code), and verifying whether such technologies were used during the transaction.
5. Behavioral indicators: Does the transaction appear unusual compared to the customer's typical behavioral patterns?
6. Account activity: Was this a one-time incident, or were there multiple unauthorized transactions associated with the customer's account?

C. After conducting the initial assessment of the fraud case based on all gathered evidential data, the Company makes its decision regarding the fraud process, which includes arriving at one of the following conclusions:

1. The complaint is groundless and no further measure is needed.
2. The case must be referred to a higher director or to the unit responsible for investigating fraud incident at the Company for further investigation.
3. The case needs the Central Bank advice, the Cybercrime Unit or any competent authority.

D. Decision on the case must be recorded together with the following:

1. The reason for the decision and its justifications.
2. The legal base according to which the decision is taken.
3. Measures to be taken (if any).
4. The identity of the person or external authority responsible for taking any subsequent measure.
5. The name and position of the person who took the decision.
6. The date of the decision.
7. The available options for addressing the fraud case, including the options related to engaging an independent third party for investigation and the required resources and expertise

E. When a decision has been made to proceed with an investigation into a suspicious fraud case, the responsible party for the investigation (the appointed committee) must develop an investigation plan that takes the following into consideration:

1. The investigation scope and conditions.
2. Identification of operational areas and key employees who will participate in the investigation.
3. Identification of required specialized expertise or support.

F. The head of the investigation team must constantly re-evaluate the investigation process and determine the need to report to other regulatory authorities, including law enforcement agencies, while keeping Senior Executive Management informed of the latest developments in the investigation.

G. Retaining all evidences related to the fraud investigation, protecting it from damage, loss, or tampering, and preserving it in secure locations, as well as keeping copies of investigation documents, while maintaining records that specify everyone who has handled these pieces of evidence.

H. Retaining fraud case reports for a period of five years in offices, and if stored electronically, these records must comply with the requirements of the electronic record as specified by the legislations in force.

I. Upon concluding the investigation, proceed with the evaluation of internal controls to prevent future fraud occurrences and take necessary measures to recover the proceeds of the fraud, if identified.

6. Financial Fraud Cases Remediation

The Company should define, approve, implement and maintain a process to identify the root cause of a fraud incident, determine any lessons learned, and take corrective actions to prevent a recurrence. In this regard, the Company is responsible for the following:

A. When seeking to identify the root cause of the financial fraud case, the Company must take the following into consideration

1. Understanding the point of deficiency/ fault/ violation (e.g., the channel that was used to perpetrate the fraud or take control of an account/ payment instrument).
2. Determining whether other parties may have been involved in the fraud (e.g., additional employees through collusion or persons known to the customer).
3. Reviewing whether a preventive control has failed or been bypassed by an employee.
4. Evaluating whether the fraud was proactively identified by a detective control or relied on reactive customer notification, third-party alerts, or notifications from relevant competent authorities, including the Central Bank.

B. Following determination of the root cause, the Company should implement appropriate mechanisms to identify lessons learned and inform corrective actions to prevent a recurrence. At a minimum the process should include:

1. Collecting data which may support the analysis of patterns in fraud cases.
2. Assessing whether there is a gap or deficiencies in the current internal control environment framework.
3. Determining whether other departments of the Company have the same vulnerability.
4. Evaluating whether the issue could affect other companies and sharing relevant information that may prevent a recurrence (e.g., fake websites impersonating government entities or social media accounts).
5. Documenting corrective actions to address the root cause and prevent a recurrence.

C. Company should take corrective actions to remediate the root cause and the impact of a fraud incident, which may include but are not limited to

1. Implementing a new rules or control, or enhancing existing ones.
2. Promoting training aspects or communicating new awareness materials to improve employee, customer or third party awareness.

3. Putting the defrauded customer back into the position they were in prior to the incident occurred based on the investigation's findings (e.g., reimbursing stolen funds).
4. Providing support to the defrauded customer (e.g., informing them of next steps, providing a new card, providing education).
5. Attempting to recover funds or assets for the benefit of the Company.
6. Terminating a customer or third party relationship if they are found to be associated with the perpetrator of a fraud.
7. Taking disciplinary action against the employee if involved in an internal fraud case, and implementing administrative measures against any third party associated with the fraud.

D. The acceptance and implementation of corrective actions should be tracked by the Counter-Fraud Department with escalation to the Counter-Fraud Committee in cases where the executive managers reject actions or remedial action is delayed.

7. Raising awareness and providing education

The Company should realize that the contribution of employees and customers in combating fraud is essential, and that most fraud cases will not be detected or monitored without their cooperation. Therefore, there is a need to increase awareness and strengthen their commitment to fraud prevention. This can be achieved through a series of ongoing initiatives, including:

A. Developing and implementing a comprehensive training program for employees to familiarize them with fraud, its various forms, methods, reporting procedures, and associated risks, the role and responsibility of each individual in the Company regarding fraud prevention and detection. Moreover, it is essential to use real-life, relevant examples (whenever possible) extracted from actual cases faced by the Company or other companies.

B. Organizing informative sessions and regular discussion forums for Company's employees on the Company's surveillance and security systems, the Counter-Financial Fraud Policy, responsibilities, ethical considerations related to fraud

prevention, code of conduct and reporting fraud cases, emphasizing that the employees' cooperation directly contributes to the effectiveness of the Counter-Financial Fraud Policy.

C. Developing periodic programs to raise awareness and educate both customers and Company's employees about various types of financial fraud, including both existing and emerging ones. These programs should take into account tools and methods that are most effective for educating each customer or employee category or group. Afterward, the effectiveness and efficiency of these awareness tools should be measured, standard indicators should be established, and necessary directions should be formulated to enhance the level of awareness regarding financial fraud.

D. Using all available and appropriate methods to convey awareness messages to the targeted groups about fraud techniques and ways to protect against them. These methods include informative brochures, text messages, visual and audiovisual advertisements, and social media platforms.

E. Monitoring and tracking information sources about emerging fraud methods and best practices to overcome them, and distributing relevant information to employees and customers.

F. Enhancing customers' awareness of the risks of financial fraud exposure and their responsibilities towards the Company in case they detect any financial fraud attempts, as well as ways to protect themselves from financial fraud.

Appendix (1): Examples of the most prominent cases of financial fraud in the National Payments System.

Appendix (2): General guidelines for customers to protect themselves from fraud risks

Appendix (1)

Examples of the most prominent cases of financial fraud in the National Payments System.

In this appendix, we highlight the most prominent indicators and patterns of financial fraud cases that have affected components of the National Payments System. These cases have been monitored, analyzed, and reported to the Central Bank by companies providing electronic payment services, or managing and operating electronic payment systems. In addition to potential cases that may arise due to the electronic nature of payment systems, tools, and channels, as well as practices in the field of electronic fraud.

Identity Theft Fraud

- Using falsified data to open bank accounts by exploiting weaknesses in the remote account opening system at the bank.
- Opening e-money accounts using false information and forged documents by exploiting weaknesses in the remote account opening system at the Company.

Electronic Wallet Fraud

In this type of channel, fraud cases usually involve using social engineering techniques to gain access to the electronic wallet owner's data and withdraw funds or use them for unauthorized transactions. Examples of fraud in this channel include:

- Fraud against customers by convincing them to transfer a financial amount through an e-wallet to the scammer's wallet under the pretense of receiving support or financial aids.
- Exploiting weaknesses or technical glitches within a Company to transfer funds between e-wallets without deducting them from the sender's account.
- Agents defrauding payment service providers by executing repeated deposit transactions to gain additional commissions.

- **Phishing links**
  - Fraudsters create a third-party phishing website that looks like an existing genuine website, such as a bank's website, an e-commerce website, or a search engine, etc.
  - Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger, etc.
  - Many customers click on the link without checking the address details (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), Password, etc., which are captured and used by the fraudsters.

- **Vishing**
  - Fraudsters call or approach the customers through phone calls / social media posing as bankers, Company executives, insurance agents, or government officials, etc. in order to gain their confidence, as fraudsters share a few customer details such as the customer's name or date of birth.
  - In some cases, fraudsters pressurize / trick customers into sharing confidential details such as passwords, OTP, PIN, or Card Verification Value (CVV) etc., by citing an emergency such as need to block an unauthorized transaction, a payment required to stop some penalty, or an attractive discount, etc. These credentials are then used to defraud the customers.

- **Fraud due to the use of unknown / unverified mobile apps.**
  - Fraudsters disseminate SMS / email / social media / instant messenger, etc., certain app links, masked to appear similar to the existing apps of authorized entities.
  - Fraudsters deceive the client into clicking on these links, leading to downloading of unknown/unverified applications on the customer's mobile phone, computer, etc.
  - Once the malicious application is downloaded, the fraudster gains full access to the client's device, including confidential details stored on the device and messages / OTPs received before / after installation of such apps.

- **Fraud through stealing payment card data via ATMs**

  - Fraudsters install skimming devices in ATMs to steal data from the customer's card.
  - Fraudsters may also install a fake keypad or a discreetly hidden small camera to capture the customer's PIN.
  - Sometimes, fraudsters may impersonate other customers, standing near-by, to observe and gain access to the PIN when the customer enters it in an ATM machine.
  - This data is then used to create a duplicate card, and withdraw money from the customer's account.

- **Fraud through Quick Response code (QR) scan**

  - The fraudsters often contact customers under various pretexts and deceive them into scanning QR codes using the applications on their mobile phones.
  - By scanning these QR codes, customers may unintentionally authorize the fraudsters to withdraw money from their accounts.

- **Lottery fraud**

  - Fraudsters send emails or make phone calls claiming that the customer has won a large lottery prize. However, in order to receive the money, the fraudsters ask the customers to confirm their identity by entering their bank account/ credit card details on a website from which data is captured by the fraudsters.
  - Fraudsters may also ask the customers to pay taxes, forex charges, upfront or pay the shipping charges, processing, handling fee, etc., to receive the lottery or product.
  - Fraudsters in some cases may also pose as a representative of the Central Bank or a foreign bank, a company, or an international financial institution and ask the customer to transfer a relatively small amount in order to receive a larger amount in foreign currency from that institution.

- Since the requested money is generally a very small percentage of the promised lottery or prize, the customer may fall into the trap of the fraudster and make the payment.

Fraud through SMS / Email / Instant Messaging / Fake Messages

- Fraudsters circulate fake messages in instant messaging apps, SMS, social media platforms on attractive loans and use the logo of any known bank or company as their profile pictures in while using the mobile number shared by them to induce credibility.
- The fraudsters may even share their fake ID Card.
- After sending such bulk messages, SMS, or emails, the fraudsters call random people and share fake sanction letters, copies of fake cheques, etc., and demand various charges. Once the customers pay these charges, the fraudsters abscond with the money.

OTP based Frauds

- Fraudsters impersonating as bank or financial institution (FI), send SMS messages offering loans or enhancement of credit limit on financial institution or bank customers' loan accounts, and ask the customers to contact them on a mobile number.
- When the customers call such numbers, fraudsters ask them to fill forms to collect their financial credentials. Fraudsters then convince the customers to share the OTP or PIN details and carry out unauthorized transfers from the customers' accounts.

Ponzi / Multi-Level Marketing (MLM) schemes fraud

- Fraudsters use Ponzi and Multi-Level Marketing (MLM) schemes (Pyramid Structure schemes) to promise easy or quick money upon enrolment or adding of members through electronic platform for this purpose.
- The schemes not only assure high returns but also pay the first few instalments to gain confidence of persons and attract more investors through word of mouth publicity.

- The schemes encourage addition of more people to the chain or the group. Commission is paid to the enroller for the number of people joining the scheme, rather than for the sale of products.
- This model becomes unsustainable after some time when number of persons joining the scheme starts declining. Thereafter, the fraudsters close the scheme and disappear with the money invested by the people till then.

Appendix (2)

General guidelines for customers to protect themselves from financial fraud risks

Customers bear a significant portion of the responsibility for protecting themselves from financial fraud, and in this regard, we provide some guidelines that customers should be aware of to safeguard themselves from falling victim to any financial fraud. Customers should always remember that financial fraud begins with their response, and avoiding financial fraud starts with not responding to any unknown party requesting their financial and personal information, no matter how trustworthy it may seem, as trust is the fraudster's weapon to reassure and convince the customer of their credibility. Companies can benefit from these guidelines when implementing their awareness programs for their customers regarding financial fraud.

Phishing links

- Do not click on unknown or unverified links and immediately delete such SMS and email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank website, e-commerce, or search engine, and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank or service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials data.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion, report it.

Precautions about vishing calls

- Officials of banks, financial institutions, the Central Bank, OR any genuine entity never ask customers to share confidential information such as username / password/ card details/ CVV/ OTP.

- Never share these confidential details with anyone, even your own family members, and friends.

Frauds due to the use of unknown / unverified mobile apps

- Never download an application from any unverified or unknown sources or on being guided by an unknown person.
- As a prudent practice before downloading, check on the publishers or owners of the app being downloaded as well as its user ratings etc.
- While downloading an application, check the permissions and the access to your data it seeks, such as contacts, photographs, etc. Only give those permissions which are absolutely required to use the desired application.

Fraud through QR code scan

- Be cautious while scanning QR codes using any payment app. QR codes may have account details embedded in them to transfer money to a particular account.
- Never scan any QR code to receive money. Transactions involving receipt of money do not require scanning barcodes, QR codes, or entering mobile banking PIN, passwords, etc.

ATM card skimming

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- Never write the PIN on your payment card.
- Do not enter the PIN in the presence of any other or unknown person standing close to you.
- Do not give your payment card to anyone for withdrawal of cash.
- Do not follow the instructions given by any unknown person or take assistance and guidance from strangers or unknown persons at the ATMs.
- If cash is not dispensed at the ATM, press the 'Cancel' button and wait for the home screen to appear before leaving the ATM.

Lottery fraud

- Beware of such unbelievable lottery or offers - nobody gives free money, especially such huge amounts of money.
- Do not make payments or share secure credentials in response to any lottery calls / emails.
- The Central Bank never opens accounts of members for the public or takes deposits from them. Such messages are fraudulent.
- Never respond to messages offering OR promising prize money, government aid and required Know Your Customer (KYC) updating to receive prize money from banks, institutions etc.

OTP based Frauds

- Never share OTP, PIN, personal details, etc., in any form with anyone, including your own friends and family members.
- Regularly check SMS, emails to ensure that no OTP was generated without your prior knowledge.
- Always access the official website of the bank, payment company, or e-wallet provider or contact the branch to avail their services and seek product and services related information and clarifications.

Ponzi / Multi-Level Marketing (MLM) schemes fraud

- Returns are proportional to risks. Higher the return, higher is the risk.
- Any scheme offering abnormally high returns (40-50%) consistently, could be the first sign of a potential fraud and caution needs to be exercised.
- Always notice that any payment, commission, or percentage of profit without the actual sale of goods / service is suspicious and may lead to a fraud.
- Do not be tempted by promises of high returns offered by entities running Multi-Level Marketing/ Pyramid Structure schemes.

For device / computer security

- Change passwords at regular intervals.

- Install antivirus on your devices and install updates whenever available.
- Always scan unknown storage drives like (USB) / devices before usage.
- Do not leave your device unlocked.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or software on your phone / laptop.
- Do not store passwords or confidential information on devices.

For safe internet browsing

- Avoid visiting unsecured, unsafe, and unknown websites.
- Avoid using unknown browsers.
- Avoid saving passwords on public devices.
- Avoid entering secure credentials on unknown websites, or public devices.
- Do not share personal information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage by ensuring the presence of two indicators (https sign, and the pad lock symbol), more so when an email or SMS link is redirected to such pages.

For safe internet banking

- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, or keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (Internet cafe, etc.) for financial transactions.
- Avoid using public Wi-Fi networks.

Factors indicating that a phone is being spied on

- Unfamiliar applications are being downloaded on the phone.
- Phone battery is draining faster than usual.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.

- An unusual surge in the amount of data consumption can sometimes be a sign that a spyware is running in the background.
- Spyware apps might sometimes interfere with a phone's shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.
- Note that text messages can be used by spyware and malware to send and receive data.

Actions to be taken after occurrence of a fraud

- Inform your bank or company directly without delay.
- Block not only the payment cards but also freeze the debit in the bank account linked to the card by visiting your branch or calling the official customer care number available on the bank's website.
- Also, check and ensure the safety of other banking channels such as Internet banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.

Precautions related to payment cards

- You should deactivate various features of payment card, online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.
- Never let the merchant take the card away from your sight for swiping while making a transaction.

For password security

- Use a combination of alphanumeric and special characters in your password.
- Keep two-factor authentication for all your accounts, if such facility is available.
- Change your passwords periodically.
- Avoid having you date of birth, wife name, car number etc. as passwords.

How do you know whether a bank or company is genuine or not?

- Check if the bank or company's name appears in the list of licensed banks and companies available on the Central Bank's website under the "Payment Systems" tab.
- The company should prominently display its license issued by the Central Bank on its website.

General precautions

- Keep the PIN, password, and credit or debit card number, CVV, etc., private and do not share the confidential financial information with banks/ financial institutions, friends or even family members.
- Avoid saving card details on websites, devices, laptop, or public desktops.
- Turn on two-factor authentication where such facility is available.
- Never open / respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.

“End”