Automated Teller Machine Instructions
No. 6/ 2018
Issued pursuant to the provisions of paragraph (4/b/5) of Central Bank of Jordan Law No. (23) of 1971 as amended and the paragraphs (3 &4) of article (37) of Banking Law No. (28) For the year of 2000, and the article (55) of Electronic Payment and money Transfer bylaw No. (111) of 2017

Article (1):

These instructions are called (Automated Teller Machine Instructions) and they are in force from the date of their approval.

Article (2):

A) Wherever they should occur herein, the following words and terms shall have the meanings assigned to each hereunder, unless otherwise connoted by the context:

Payment services provider	:	The bank, the Islamic bank, or the company licensed by the Central Bank to practice the activity of managing cash deposits and withdrawals electronically through automated teller machines.
Automated Teller Machine (ATM)	:	Electromechanical machines that allow users to perform financial and / or non-financial transactions on their accounts using payment instruments or any other means.
User	:	It is any person who carries out financial or non-financial transactions through an ATM, whether he is a customer or non-customer of the payment service provider

Issuer of the payment instrument		A company licensed by the Central Bank to practice the activity of issuing and managing payment instruments.
Customer		The natural or legal person to whom the issuer of the payment instrument issues any of the payment instruments.
System operator		The company licensed by the Central Bank to practice managing and operating ATM payments clearing systems.

B) The definitions stated in the effective Banking Law and The Electronic Payment and Money Transfer Bylaw shall be adopted wherever they are stipulated in these instructions unless the context indicates otherwise.

General Scope

Article (3):

These instructions are applied to:

A) Companies operating in the Kingdom, including branches of foreign companies licensed by the Central Bank to practice the activity of managing cash deposits and withdrawals electronically and / or issuing and managing payment instruments and / or practicing management and operation of ATM payment clearing systems.

B) Banks operating in the Kingdom in a manner that does not conflict with the Banking Law and the bylaws and instructions issued pursuant thereto.

Conditions for installing ATMs

Article (4):

A) The payment service provider must take into consideration the following procedures and controls when installing an automatic teller machine (ATM):

1) Fixing the automatic teller machine in a way that hinders its removing incase the ATM is located inside and / or outside buildings, with the exception of ATMs located in public places, for example, but not limited to airports, shops and commercial complexes.
2) Hiding all electrical connections, communications cables and ports for ATMs, so that they are protected in a safe way that is difficult to be accessed except by the concerned persons, regardless of their whereabouts, especially those in public places such as airports, shops and commercial complexes.
3) Provide two network lines for the ATM from different providers.
4) Avoid installing and / or placing ATMs in unprotected locations.
5) In the case that ATMs are installed inside public places, all necessary security standards must be concerned at the ATM site.
6) Installing a satellite tracking chip (Global Positioning System chip) inside ATMs installed in public places and outside the branch buildings, enabling it to locate the device in the event it is removed, so that the tracking device is installed in a safe place inside the ATM that is difficult to be accessed.

7) Ensure that there are surveillance cameras for the ATM that show both the body of the ATM, the user for it, and the car registration plate in case the ATM provides cash withdrawal at a drive-thru ATM without showing the keypad of the ATM machine.
8) Store the images captured by the ATM surveillance cameras for an appropriate period of time, not less than one year.
9) The user has the right to view the images captured by the surveillance cameras if the need arises and according to the policies followed by the payment service provider.
10) The ATMs must be equipped with an alarm system that is directly linked to the central alarm system of the payment service provider and those responsible for these devices in addition to a detector of vibrations, frequencies and abnormal temperature, where its function is to detect any attempts to tamper with the ATMs, including cases of theft and emergency situations such as fire, and connecting the network of the payment service provider to the network in the police operation rooms or early warning stations licensed by the security services.
11) Provide a cover for the ATM keypad (Pin Shield) that prevents showing the (PIN) when entering it by the user the cover is of a type that provides privacy and protection to cover both sides of the keypad and the top side.

B) The payment service provider is obligated to supply and install ATMs that comply with all security and protection standards issued by the Electronic Payment Card industry

Security Standards Council (PCI-SSC) in terms of software and hardware and in compliance with the conditions and requirements mentioned in these instructions as a minimum.

Technical and ecurity conditions that must be applied to ATMs

Article (5):

The payment service provider must adhere to the following security and supervisory controls as a minimum:

A) Plating the card reader to protect it from any external penetration.

B) Determine the permissions of those authorized to access ATMs and the supporting systems in accordance with the procedures specified by the payment service provider in this regard, and review and update those permissions continuously.

C) It is imperative that no part of the ATM machine be opened except in the presence of dual control by persons authorized by the payment service provider.

D) Ensuring the security of the cash dispenser on the ATM to prevent the entry of any unknown object inside it for the purpose of theft or fraud.

E) Documenting all developments and changes that are made to the hardware and software of ATMs to prevent any unauthorized actions on these devices.

F) The necessity of stopping the operation of the ATM machine in the event that any counterfeiting device connected to the ATM is discovered or tampering with it is discovered until the problem is resolved.

G) Recording of events that take place on the operating system of the ATM through incident and event records and monitoring them, preventing these records from being modified or deleted by unauthorized persons and documenting this.

H) When dispensing with an ATM, the sensitive information and components on it must be deleted in a way that cannot be retrieved later, with the necessity to store the devices intended for destruction in a safe place designated for this purpose until they are destroyed.

I) To meet the specifications of the ATM Safe, so that they align with the (CEN1) standard at the minimum, and the payment service provider is obligated to reconcile their status in compliance with this clause within a period of three years from the date of issuance of these instructions.

Article (6):

The payment service provider must adhere to the following as a minimum with regard to protecting ATM networks:

A) That the payment service provider's ATM network be protected by being Segmented from the network of its systems.

B) The communication mechanism used within the ATM and between the payment service provider's ATM network and its systems and the system operator is secure, encrypted and use highly reliable algorithms that are not easily decipherable.

Article (7):

The payment service provider must adhere to the following as a minimum with regard to protecting the data of the payment instrument and the data used to perform operations on the ATM:

A) The ATM card reader contains the appropriate tools to prevent skimming the card data, for example but not limited to, the use of an anti-skimming card reader which uses the jamming signal / noise disruption mechanism, and that the software installed on it be updated to this purpose in a continues manner.
B) The data entered through the keypad of the ATM and transmitted within the ATM and between the ATMs and the payment services provider's systems must be encrypted using highly reliable algorithms that are not easily decipherable.
C) The hard disk in ATMs must be fully encrypted using highly reliable algorithms that are not easily decipherable to ensure the safety of the data and programs stored on it from any penetration, and to protect the ATM system from any malicious programs that may be exposed to it.
D) Printing the authorization number for the operation that was performed through the ATMs on the receipts extracted from it.
E) The card data, its number, expiration date, and / or the name of the cardholder must not be printed on receipts extracted from ATMs.

Article (8):

The payment service provider must adhere to the following as a minimum with regard to protecting the systems and software installed on the ATM:

A) Ensure that anti-virus and anti-spyware programs, as well as any adequate applications and protection software are installed on the ATMs and are continuously updated.

B) Ensure that the operating systems and software installed on the ATMs are continuously updated.

C) Not to update or install programs and applications on ATMs remotely through the Remote Desktop Protocol (RDP) in any way.

D) Put settings for the BIOS program (Basic Input Output System) installed on the ATM in a way ensure that the ATM machine is running from the hard disk only, preventing any automatic updates to the BIOS program, in addition to having a password to enter the settings of this program.

E) Applying a strong policy for the password used to enter the BIOS program and used for the accounts of users of operating systems of ATMs that prevent others from breaking it, determining, for example, the length of the password and the nature of the codes used in it, taking into account that it is continuously updated and not repeated, etc.

F) Delete any unnecessary and unused applications and software on the ATM to reduce the possibility of any hacking or cyber attack on these applications and software.

G) Disable the auto-play feature on the ATM's operating system, which automatically runs programs installed on any storage media such as CD, DVD or USB flash when inserted on the ATM to prevent the possibility of malicious programs running automatically through them.

H) Using a mechanism to excute the orders defined for the ATM’s operating systems only (White listing) and updating those orders continuously, in order to protect against the execution of orders belonging to the malicious programs, in addition to obtaining a feature to send automatic alerts in case that the program stops or objects to the execution of an order that is not defined for it.

Managing and Controlling the ATMs

Article (9):

The payment service provider has must have a specialized unit to manage and control all ATMs, so that its tasks include, as a minimum, the following:

A) Coordination with all branches of the payment service provider, its organizational units, and any other related parties, regarding the management and control of ATMs and their operations.

B) Ensure the operation of ATMs and their support systems all the time (24/7) and ensure the continuity of their work, except in cases where ATMs experience technical malfunctions or interruptions in network communications that are difficult to solve in real time.

C) Addressing the reasons for stopping services at ATMs other than scheduled maintenance and feeding operations, or any reason out of control or the existence of a technical defect that could not be addressed by the payment service provider or the supplier within a maximum of 48 hours from the moment of discovering that the service is not available.

D) Inspecting the ATMs and their supporting components such as network devices and communication cables, at the minimum every three days, and make sure that there are no non-trusted or suspicious devices or equipment on the ATM, such as a card skimmer, card reader, cameras to detect the password or illegal tampering attempts.

E) Conducting a penetration test to examine the security vulnerabilities in the ATMs and the ATM network of the

payment service provider by a competent entity at least once annually and whenever substantial modifications are made.

Users Protection

Article (10):

The issuer of the payment instrument must adhere, as a minimum, to the following:

A) Immediately inform his customer about the financial operations that have been executed on his accounts using ATMs, using an effective and clear communication method in both Arabic and English languages such as SMS, provided that it includes at least the place, date and time of the transaction, its value and the type of currency.

B) Immediately suspend payment instruments if the customer reported about the loss or breach of his payment instrument.

C) Take out the user's card and alert him to take it more than once and for a certain period of time, and if the user does not take it, the card is taken and confiscated by the ATM as a security precaution.

D) Reject the card used on the ATM in case the card is expired or reported as lost, dormant, canceled, or not in conformity with security specifications or any other reason and inform the user through the screen of the ATM about the reason for rejecting the card.

E) Ensure that the customer's mobile phone number is registered and updated for the purpose of notifying the customer of the execution of any financial transaction on the ATM immediately.

Article (11):

The issuer of the payment instrument and the payment service provider must continuously educate users / customers on the secure practices for using ATMs to avoid fraud and maintain the privacy of payment instrument data and passwords related to it, provided that it includes, at a minimum, the following:

A) Executing his operations on ATMs in complete privacy.
B) Not to lend the payment instruments to anyone.
C) Not to write the password on the card used on the ATM.
D) Not to disclose the password to anyone.
E) Not to allow anyone to see the password when entering it on the ATM.
F) Ensure to take the payment instrument from the ATM after completing any transaction on it.
G) Inform the issuer of the payment instrument in the event that the customer loses his payment instrument or if the customer discovers that financial transactions have been executed on his accounts through ATMs by someone other than him.
H) The user has the right to object to the transactions executed on his accounts through the ATM within a period of (60) days from the date on which he was notified of the transaction data by the issuer of the payment instrument or whoever authorized him.

System operator obligations

Article (12):

The system operator must integrate the ATM payment clearing system with the real time gross settlement system - Jordan (RTGS- JO) at the Central Bank to settle the net financial positions of all payments made on ATMs locally through bank accounts, and he is also obligated to provide special guarantees

during The time limit, arrangements and procedures that are determined and announced by the Central Bank at a later time.

General Provisions

Article (13):

A) The payment service provider is obligated to notify the Central Bank of any hacking or fraud cases that may occur on ATMs within a maximum of 72 hours from the moment the event is discovered.

B) The payment service provider must immediately take the following measures once he detects that a hack has occurred on an ATM:
   1) Suspending all payment instruments issued by him and used on the ATM that was hacked or fraudulent and during the estimated period of the breach.
   2) Reporting to the system operator to inform him of the breaches or fraud that occurred on his ATMs, so that he would address the issuers of the payment instruments used on those machines in order to suspend them.

C) Payment service providers and issuers of payment instruments are obligated to follow all circulars issued by the Central Bank regarding the latest cases of fraud that occurred at ATMs and the procedures that must be followed by them to avoid the occurrence of such cases.

Article (14):

Payment service providers are obligated to provide the Central Bank with a statistic indicating the number of ATMs, their locations, the services they provide, the volume and values of the

transactions executed through them, and the fraud cases they have been exposed to according to the forms designated for that and according to the periodical specified by the Central Bank to be appropriate.

Article (15):

Payment service providers are obligated to adjust the status of their ATMs within a year from the date of issuing these instructions, taking into consideration Article (5 / I) of these instructions.

Article (16):

Payment service providers, Issuers of payment instrument, and system operator must comply with all security and protection standards issued by the Electronic Payment Card Industry Security Standards Council (PCI - SSC).

Article (17):

In case that the provisions of these instructions are violated, the Central Bank may apply the penalties stipulated in the legislations governing the bodies subject to the provisions of these instructions, as required by the case.

Governor
Ziad Fariz