BANK OF PAPUA NEW GUINEA

DIRECTIVE ON ELECTRONIC FUND TRANSFERS 02/2019

PART I

PRELIMINARY

1. Scope

(1) In accordance with principles and rules laid down in the National Payments System Act (NPS) 2013 and within the powers of the Central Bank granted by Article 3 this Directive legalises its enforcement, as well as rights and/or obligations in the provision of transfers executed, either totally or partially, by electronic or any other automated means (generally referred to as "**electronic fund transfers**"). These can be either payments originated by the payer (credit transfer) or the payee (direct debit), or money transactions.

(2) This Directive establishes the rules to protect persons being the users of payment instruments and facilities employing electronic devices or facilities.

(3) Electronic fund transfers include those carried out through or by means of, or a combination of the following:

(a) Point-of-sale (POS) terminals;
(b) Automated teller machines (ATM);
(c) TV, internet and other communication channels;
(d) Telephonic instruments, including mobile phones;
(e) Cards; and
(f) Card-based and network-based stored value products/devices (e-money).

(4) This Directive shall apply to single electronic fund transfers, as well as to framework contracts and transfers covered by them.

2. Definitions

For purposes of this Directive, unless the context otherwise requires:

- "Account" means any account maintained with an institution permitted to do so by the Central Bank and duly supervised;

- "Card" means a device, including an ATM, POS, debit, credit, virtual or stored value card, as defined and regulated by Central Bank from time to time, that can be used by its holder to effect an electronic fund transfer;

- “Customer” means a person or entity using an electronic device or facility to execute electronic fund transfers;

- “Electronic consent” means any sound, symbol, or process which is:

(a) related to technology (i) having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities, including (but not limited to) mobile telephony, facsimile and internet and (ii) which may only be accessed through a security access code, and
(b) logically associated with a legally binding agreement or authorization and executed or adopted by a person with the intent to be bound by such agreement or authorisation;

- “Electronic fund transfers system” means a wire transfer network, automated clearing house (ACH), or other systems or arrangement for the processing, clearing and/or settlement of electronic fund transfers;

- “Framework contract” means a contract which governs the future execution of individual and successive electronic fund transfers and which may contain the obligation and conditions for setting up an account to execute such transfers;

- “Money transaction” means the deposit or withdrawal of cash or any other transfer of money not representing a payment;

- “Payee” means the person who is the intended final beneficiary of funds in an electronic fund transfer;

- “Payee payment institution” means the payment service provider identified in a payment order which is to make payment to a payee:

(a) by crediting the account of the payee; or

(b) in any other manner, where the payment order does not provide for crediting an account;

- “Payer” means a person who holds an account and allows a payment order by debiting that account; or, where there is no account, a person who originates a fund transfer to the benefit of a payee;

- “Payment order” means a payment instruction by a sender to a sender’s payment service provider, transmitted electronically, or in writing, to pay, or to cause another payment service provider to pay, a fixed or determinable amount of money to a payee if:

(a) the instruction does not state a condition of payment to the payee other than time of payment; and

(b) the instruction is transmitted by the sender directly to the sender’s payment service provider or to an agent, electronic fund transfers system or communication system for transmittal to the sender’s payment service provider.

- “Preauthorised electronic fund transfer” means any prior arrangement or agreement between a customer and an institution to authorise it to:

(a) make payments to a third party out of the funds standing in the account of the customer; or

(b) transfer funds from one account of the customer to another account of the customer maintained with the institution or another institution.

- "Security Access Code" means a personal identification number (PIN), password, code or any other device or mechanism providing a means of certified access to a customer's account for the purposes of, among other things, initiating a electronic fund transfer;

- "Security procedure" means a procedure established by agreement of a customer and a payment service provider for the purpose of:

(a) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or
(b) detecting error in the transmission or the content of the payment order or communication.

A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, call-back procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.

- "Sender" means the originator of a transfer, this being either a payer or a payee as the case may be.

PART II

REGULATORY ASPECTS

3. Duties of Payment Service Providers

(1) Payment service providers offering electronic funds transfers by any means are responsible to ensure compliance to this Directive for their own acts and for the acts of any third party contracted by them to provide services linked to the execution of electronic fund transfers or the provision of connected services to the customers.

(2) In particular, payment service providers may use the services of agents and shall adhere to all applicable laws and Directives on appointing and obtaining the services of such agents.

(3) Payment service providers shall have a proper system for registration of customers before providing electronic fund transfers and shall not impose the use of individual channels or products unless the customer has subscribed to it.

(4) They shall have a comprehensive risk management framework that clearly identifies and mitigates any channel/service specific risks. Such measures shall be approved by the board of the relevant payment service provider.

(5) In conformity with and by no derogation to the Banks and Financial Institutions Act 2000, banks are allowed to open limited-purpose and no-interest bearing accounts for the execution of electronic fund transfers by channels and mechanisms like for (e.g.) ATMs,

agents, POS terminals, mobile phones, kiosks and other such devices, under specific conditions as established by the Central Bank.

4. **Technology and Information Security Standards**

(1) The technology used for supplying payment service facilities for electronic transfers must be safe and secure and shall ensure confidentiality, integrity, authenticity and non-repudiation of the payment related information.

(2) In order to ensure implementation of paragraph (1) above, the Central Bank may publish best practices and guidelines as deemed necessary from time to time.

(3) Payment service providers shall update and implement the information security policy to adequately address the security requirements of the relevant delivery channels.

(4) Payment service providers shall use methods consistent with industry best practices to authenticate user identity.

(5) Payment service providers shall provide controls that allow customers the ability to receive payment alerts and notices in accordance with their preference.

(6) Payment service providers shall implement a robust security risk management framework to actively identify, assess, reduce and monitor security risk. The security system shall ensure:

(a) Confidentiality of the sensitive information. All confidential information shall be maintained in a secured manner and protected from unauthorized viewing or modification during transmission and storage;
(b) Accuracy, reliability and completeness of information processed, stored or transmitted;
(c) Proper authentication of users and agents;
(d) Proper authorization of functions performed by users and agents;
(e) Online transaction monitoring to detect fraudulent transactions and promptly act on them; and
(f) Risk controls at all points involving interactions with customer and exchange of sensitive information and changes to product/service attributes.

5. **Interoperability**

When a payment service provider offers electronic fund transfer services that rely on general purpose electronic devices, software or service not provided by the payment service provider to the subscriber, they shall ensure that any customers be in a position to request for and avail such services, irrespective of their choice of the provider providing the electronic device, software or service.

6. **Customer Protection**

(1) Payment service providers shall provide the terms and conditions applicable for the utilisation of electronic fund transfer services in an appropriate manner in websites, brochures and registration forms. These terms and conditions should be unambiguous and shall consist of following, inter alia:

(a) Authorised types of payments;
(b) Rights and responsibilities of the service provider, account holders and agents with regard to electronic fund transfer services (or the specific category offered);
(c) All applicable fees and charges;
(d) Benefits, incentives and rewards;
(e) Provisions for dispute resolution;
(f) Procedure for reporting lost or stolen payment instrument or device;
(g) Procedure for stop payments; and
(h) Customer service contact numbers.

(2) Payment service providers shall ensure that terms and conditions on electronic fund transfer operations shall not vary, amend or modify in any manner except by a prior notice to the customers, through appropriate communication media.

(3) Payment service providers shall maintain the confidentiality of customer information and shall be responsible to ensure that any contracted third party service provider will also treat customer information as confidential. They shall institute appropriate and adequate risk control measures to manage the risk of liability to the customers on account of breach of secrecy, for which the service provider may be exposed due to the high level of information security risk associated with electronic fund transfers.

(4) Payment service providers shall enter into commercial contracts with any third party service providers possibly involved in the provision of the service, in addition to the agreements with account holders who subscribe for electronic fund transfer services. The rights and obligations of each party shall be made clear through these contracts and shall be valid and enforceable in a court of law.

(5) Payment service providers shall adhere to the laws and Directives applicable to the security procedure adopted to authenticate users as a substitute for signature, when providing electronic fund transfer services to account holders.

(6) Payment service providers shall educate customers on applying security features and capabilities and the importance of protecting their personal information.

PART III

PROCESSING OF ELECTRONIC FUND TRANSFERS

7. Execution

(1) A payment service provider shall execute a payment order originated by a payer immediately upon receipt unless otherwise instructed by the sender; provided, however, in no event shall the payment service provider be obligated to execute the payment order if there are insufficient funds in the account from which the funds are to be transmitted.

(2) The payee's institution shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's institution's account.

(3) In the evaluation of the immediacy of execution, rules of electronic fund transfer systems through which the order is processed shall be taken into account. Fund transfers originated by the payer shall in any case be finally made at the disposal of the payee within 24 hours from initiation of the transfer.

(4) In case of a payment order initiated by or through the payee, the payee's payment service provider shall transmit it to the payer's payment service provider within the time limits agreed between the payee and his payment institution, enabling settlement, as far as direct debit is concerned, on the agreed due date.

8. Receipt of Payment Orders

(1) The point in time of receipt is the time when the payment order from the payer or the payee is received by the payer's payment institution.

(2) The payer's payment institution may fix a cut-off time or times on a business day for the receipt and processing of payment orders. Different cut-off times may apply to payment orders, or to different categories of payment orders. A cut-off time may apply to senders generally or different cut-off times may apply to different senders or categories of payment orders.

(3) If a payment order is received after the close of a business day or after the appropriate cut-off time, the payment service provider may treat the payment order as received at the opening of the next business day.

9. Irrevocability

(1) The payer may not revoke a payment order once it has been received by the payer's payment institution, unless otherwise provided by agreement.

(2) Where the payment order is initiated by or through the payee, the payer may not revoke the payment order after transmitting the payment order or giving his consent to execute the payment transaction to the payee.

(3) Any derogation to paragraph (2) shall be clearly spelled out in the agreement regulating the terms of mandate and shall not prejudice the application of Section 20 of this Directive on right to refund.

(4) Rules applicable to payment orders shall equally apply to communications cancelling or amending a payment order.

10. Transmission of payment orders through electronic fund transfers or other communication system

(1) If a payment order addressed to a payment service provider is transmitted to an electronic fund transfers system or other third-party communication system for transmittal to the institution, the system is deemed to be an agent of the sender for the purpose of transmitting the payment order to the institution. If there is a discrepancy between the terms of the payment order transmitted to the system and the terms of the payment order transmitted by the system to the institution, the terms of the payment order of the sender are those transmitted by the system, unless otherwise provided by the rules of the system.

(2) A bank or other payment service provider shall not avoid any obligation to its customer by reason only of the fact that it is a party to a shared electronic fund transfers system, and that another party to the system had failed to fulfill its obligations under this Directive.

(3) The respective rights and responsibilities of parties to a shared electronic fund transfers system shall be determined by bilateral or multilateral agreement of parties.

PART IV

UNAUTHORISED AND ERRONEOUS FUND TRANSFERS

11. Authorization of Transfers

(1) An electronic fund transfer is considered to be authorized only if the sender has given consent to execute such transfer.

(2) Consent to execute an electronic fund transfer or a series of transfers shall be given in the form agreed between the parties.

(3) In the absence of such consent, a transfer shall be considered to be unauthorized.

(4) If a bank or other payment service provider and its customer have agreed that the authenticity of payment orders issued to the bank or the payment service provider in the name of the customer as sender will be verified pursuant to a pre-agreed security procedure, a payment order received by the receiving institution is effective as the order of the customer, whether or not authorized, if:

(a) The security procedure is a commercially reasonable method of providing security against unauthorized payment orders; and

(b) The institution proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The institution is not required to follow an instruction that violates a written agreement with the customer or notice of which is not received at a time and in a manner affording the institution a reasonable opportunity to act on it before the payment order is received.

(5) Schedule 3 of the Oversight Directive shall determine the appropriate size, type and frequency of the payment orders by customers and payment service providers and apply to this Directive.

12. Erroneous Payment Orders

(1) If a payment order was transmitted pursuant to a security procedure for the detection of error, and the payment order:

(a) Erroneously instructed payment to a payee not intended by the sender;

(b) Erroneously instructed payment in an amount greater or lower than the amount intended by the sender, or

(c) Was an erroneously transmitted duplicate of a payment order previously sent by the sender,

(d) the following rules apply:

(i) If the sender proves that the sender or a person acting on behalf of the sender complied with the security procedure and that the error would have been detected if the receiving institution had also complied, the sender is not obliged to pay the greater order to the extent stated in (ii) and (iii) of this subsection.

(ii) If the transfer is completed on the basis of an erroneous payment order described in (a) or (c) of this subsection, the sender is not obliged to pay the order and the receiving institution is entitled to recover from the payee any amount paid to the payee to the extent allowed by law.

(iii) If the transfer is completed on the basis of a payment order described in (b) of this subsection:

1. In case the amount received by the payee is greater than the amount intended by the sender, the sender is entitled to recover from the payee the excess amount received to the extent allowed by law; and
2. In case the amount received by the payee is lower than the amount intended by the sender, the sender has to pay the difference to the payee.

(2) If (a) the sender of an erroneous payment order described in subsection (1) is not obliged to pay all or part of the order, and (b) the sender receives notification from the receiving institution that the order was accepted by the institution or that the sender's account was debited with respect to the order, the sender has a duty to exercise ordinary care, on the basis of information available to the sender, to discover the error with respect to the order and to advise the institution of the relevant facts within a reasonable time, not exceeding ninety days, after the institution's notification was received by the sender. If the bank proves that the sender failed to perform that duty, the sender is liable to the institution for the loss the institution proves it incurred as a result of the failure, but the liability of the sender may not exceed the amount of the sender's order.

The payer's service provider shall be responsible for any incorrect amount received by the payee in connection with the payment order.

13. **Notification of loss, theft or unauthorized use**

(1) A payment service provider shall provide an effective and convenient means by which a customer can notify any loss, misuse, theft or unauthorized use of a card or other electronic device or breach of a security access code.

(2) A payment service provider shall provide procedures for acknowledging receipt of notifications, including telephone notification, by a customer for any loss, misuse, theft or unauthorized use of a card or other electronic device or breach of access code security.

(3) The acknowledgment needs not be in writing provided the institution has a means by which a customer can verify that he had made a notification and when such notification was made.

14. **Liability in cases of system or equipment malfunction**

(1) A payment service provider shall be liable to its customer:

(a) For a loss caused by the failure of an electronic fund transfer system or equipment to complete a transaction accepted by a terminal, in accordance with the customer's instruction; or

(b) For computing or book keeping error made by the institution.

(2) A payment service provider shall inform a customer immediately through:

(a) Notice at ATM, POS or other electronic terminals; and

(b) Notice at its branches; or

(c) Any other mode it has been agreed with the customer, if it is aware that the system or equipment to carry out electronic fund transfer is not available for use or where there is a malfunction.

(3) The payment service provider shall inform immediately the customer of any occurred failure in the execution of a payment order for any previously undetected malfunctioning of the system.

(4) Where the customer should have been aware that the system or equipment was not available for use or malfunctioning, the service provider's responsibilities are limited to the correction of any error in the customer's account, and the refund of any charges or fees imposed on the customer for that transaction.

(5) Notwithstanding what established in subsection (4), a bank or other payment service provider shall not be liable to its customer if the failure to carry out an electronic fund transfer was caused by or resulted from force majeure or other circumstances beyond its control, provided the service provider had exercised reasonable care and diligence.

15. **Security of deposits at electronic terminal**

(1) The security of a deposit received at an electronic terminal shall be the responsibility of the institution receiving the deposit, from the time the transaction is completed, subject to verification of amount deposited.

(2) Where there is a discrepancy between the amount recorded as having been deposited at an electronic terminal and the amount recorded as having been received, the institution shall notify the customer of the difference on the next working day and shall advise the actual amount which has been credited to the customer's account.

16. **Duty of customers to notify errors**

(1) A customer shall notify his payment service provider of any error in his statement of account or possible unauthorised transaction in relation to his payment instrument, account and/or security access code.

(2) The notification shall be made in writing within twenty-eight days from the date of the statement of account.

(3) Where there is a complaint of an unauthorized electronic fund transfer by a customer, the burden of proof is on the institution to show that the electronic fund transfer was authorized.

(4) The burden of proof in subsection (3) shall be satisfied if the institution proves that:

(a) The security access code, card or other electronic devise permitting electronic consent was fully functional on that day; and

(b) The officers of or agents appointed by the institution were not fraudulent or negligent in carrying out the electronic fund transfer.

(5) For the purposes of this article, error in statement of account includes:

(a) An incorrect electronic fund transfer to or from the customer's account; or

(b) An addition or omission in the periodic statement of an electronic fund transfer affecting the customer's account.

17. **Other duties of customer**

(1) A customer shall not:

(a) Directly or indirectly disclose to any person the security access code of his card or any electronic device or software used to effect an electronic fund transfer or give electronic consent; or

(b) Fail to take reasonable care to keep the security access code or other electronic device or software secret.

(2) A payment service provider is discharged from any liability if it is proven that the customer has breached the duty imposed by subsection (1).

(3) A customer shall not be liable for losses resulting from an unauthorized transaction occurring after he has notified the bank that his card has been lost, misused or stolen, or that the security access code or other electronic device to permit electronic consent has been breached.

(4) Paragraph (3) shall apply to electronic money/stored value products except where the payer's payment service provider does not have the ability to freeze the payment account or block the payment instrument.

18. **Delay in notification**

(1) Where the customer has contributed to a loss resulting from an unauthorized transaction by delaying notification of loss, misused or theft of the card, or someone else knowing the security access code of the card or other electronic device, the customer is liable for the actual loss which occurred, except for:

(a) That portion of the loss incurred on any one day which exceeds the daily transaction limit applicable to the card, other device or account; or

(b) That portion of the total loss incurred which exceeds the amount of funds standing in the customer's account.

19. **Circumstances where customer is not liable**

(1) A customer shall not be liable for loss:

(a) Not attributable to or not contributed by the customer;

(b) Caused by the fraudulent or negligent conduct of officers of or agents appointed by:

(i) The institution;

(ii) Companies and other institutions involved in networking arrangements: or

(iii) Merchants who are linked to the card or other communication system;

(c) Relating to a card or device or software that is forged, faulty, expired or

(d) Occurring before the customer has received his card or security access code or software.

(2) Where any dispute arises in relation to a customer's card, it is to be presumed that the customer did not receive the card, unless the institution can prove otherwise.

20. **Right to refund**

(1) A payer shall be entitled to a refund from his payment institution of an authorized fund transfer initiated by or through a payee which has already been executed, if the following conditions are met:

(a) The authorization did not specify the exact amount of the payment transaction when the authorization was made; and

(b) The amount of the payment exceeded the amount the payer could reasonably have expected taking into account his previous spending/usage pattern, the conditions in his framework contract and relevant circumstances of the case.

(2) The refund shall consist of the full amount of the executed transfer. However, the payer and his payment institution may agree in the framework contract that the payer is entitled to a refund even though the conditions for refund in subsection (1) are not met.

(3) It may be agreed in the framework contract between the payer and his payment institution that the payer has no right to a refund where he has given his consent to execute the transfer directly to his payment service provider and, where applicable, information on the future transfer was provided or made available in an agreed manner to the payer for at least four weeks before the due date by the payment institution or by the payee.

(4) The payer can request the refund referred to in subsection (1) of an authorized transfer initiated by or through a payee for a period of eight weeks from the date on which the funds were debited.

(5) Within twenty-eight business days of receiving a request for a refund, the institution shall either refund the full amount of the transfer or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter if he does not accept the justification provided.

PART V

STANDARD TERMS AND CONDITIONS AND RECEIPT

21. Terms and Conditions

(1) A payment service provider providing any type of electronic fund transfer shall have standard terms and conditions in relation to the carrying out of such electronic fund transfers.

(2) The standard terms and conditions shall be in writing and in clear, readily understandable and user friendly manner.

(3) The standard terms and conditions shall be disclosed by an institution to a customer before the electronic fund transfer is carried out.

(4) The standard terms and conditions to carry out an electronic fund transfer shall include:

(a) The customer's liability for any unauthorized electronic fund transfer and duty to report to the institution promptly any loss, misuse, theft or unauthorized use of, access code or a card;

(b) The telephone number, email identity, and address of the department in charge of electronic fund transfers of the institution to be notified in the event the customer believes that an unauthorized electronic fund transfer has been or may be affected;

(c) The customer's right to stop payment of a preauthorized electronic fund transfer and the conditions and procedures to initiate such stop payment order;

(d) The maximum execution time for any kind of transfer to be executed;

(e) All charges payable by the customer and, where applicable, the breakdown of the amounts of any charge;

(f) Information relating to lodgment of complaints, investigation and resolution procedures;

(g) The customer's right to receive relevant documents in relation to electronic fund transfers; and

(h) If multiple currencies are involved, the exchange rate applied, or the method to be used to establish it.

(5) The instruction of a customer to stop payment of a preauthorized electronic fund transfer as mentioned under subsection (4)(c) shall operate immediately unless agreed otherwise by the customer and payment service provider whereby a date or time is predetermined.

22. **Availability of the terms and conditions**

(1) A payment service provider shall make available copies of the standard terms and conditions at its branches that provide electronic fund transfer services, website and any other point of access to services by customers.

(2) The payment service provider shall not charge customers for providing information referred to in subsection (1).

23. **Changes in the terms and conditions**

(1) A payment service provider may vary or modify the standard terms and conditions of an electronic fund transfer in relation to:

(a) Imposing or increasing charges;

(b) Increasing the customer's liability for losses; or

(c) Adjusting the transaction limits on the use of a card,

provided such changes are approved by the Central Bank or any other body, authorized by the Central Bank and it gives prior written notice to the customer.

24. **Notification of other changes**

(1) A payment services provider may notify the customer of any other changes in the standard terms and conditions through:

(a) Notice in the periodic statement of account;

(b) Notice at ATM, POS or other electronic terminals;

(c) Notice at its branches; or

(d) Any other mode it deems is equivalent to the above and ensures no dilution in users ability to take note.

(2) Where notification is given under subsection (1)(b), (c) or (d) and the customer is not notified directly, subsequent written advice shall be provided to the customer by the institution.

(3) Notwithstanding subsection (1), advance notice need not be given when changes are necessitated by an immediate need to restore or maintain the security of an electronic fund transfer, an electronic fund transfer system or an individual account.

25. **Records and issuance of receipts**

(1) Unless it is otherwise agreed, at the time of a payment order, the payment service provider shall ensure that a receipt is issued to the customer containing all of the following information:

(a) The amount of the transfer;

(b) The date and time (if practicable) of the transfer;

(c) The type of transfer;

(d) An indication of the account(s) being debited or credited;

(e) Data that enable the bank or other payment service provider to identify the customer and the transfer;

(f) Where possible, the type and general location of any institution equipment used to make the transaction or a number or symbol that enables that institution equipment to be identified;

(g) The name of the payee, if any, to whom payment was made;

(h) Where possible, and where it is not likely to compromise the privacy or security of the payer, the balance remaining in the account which is debited in the fund transfers (or, in the case of a deposit, the account which is credited); and

(i) Where relevant, exchange rate applied.

(2) If a payment order is given by voice communications (including an automated voice response system by telephone), the payment service provider shall ensure that the following information is provided to the customer by voice communication at the time of the order:

(a) A receipt number;

(b) The amount of the transfer;

(c) The type of transfer;

(d) An indication of the account(s) being debited or credited;

(e) The name of the payee, if any, to whom the payment was made; and

(f) Where possible, and where it is not likely to compromise the privacy or security of the customer, the balance remaining in the account which is debited in the fund transfers (or, in the case of a deposit, the account which is credited).

(3) Payment service providers may choose to provide users of the service with the option to specify at the time of each transfer that a receipt is not required.

(4) Receipts can be in electronic format, provided that these can be either stored or printed by the customer.

(5) A charge may not be imposed on a user for the issuing of a receipt under subsections (1) and (2).

(6) In case an institution's equipment may not be in a position to print receipts, the user should be notified that receipt shall not be provided on the spot, before processing the transfer, so that the user can make an informed decision whether to continue the transfer without receipt.

26. **Evidentiary value of receipts**

(1) In any legal action, the receipts issued under article (21) which indicates that a transfer was made, shall be admissible as evidence of such transfer and shall constitute prima facie proof that this was made in accordance with Article 24 of the National Payments System (NPS) Act 2013 and its implementing measures.

27. **Specific requirements for direct debits**

(1) The payer will need to provide a general mandate to the payee for periodical direct debits and one-off direct debits. The process for handling of these mandates would be specified in the rules of the payment system that processes the direct debits. The requirements in this Directive shall always prevail over such rules.

(2) In case of pre-authorized periodical direct debits, cancellation by the payer without prior notice to the payee shall be prohibited. The relevant mandate shall establish a reasonable time for the payer to inform the payee of withdrawal of given authorization, which shall only apply for the future.

(3) In conformity with Article 21(5) above, once the payer and the payee mutually terminate pre-authorized periodical direct debit arrangements, or such arrangement expires, the payer has automatic and immediate right to dishonor payments.

(4) The payer can stop transfer orders for payments that exceed an amount and periodicity reasonably expected to be collected by the payee under a specific mandate.

(5) The rules under this Article shall complement all other provisions applicable to the payee when the order is originated by the payee itself as contained in this Directive.

PART VI

INVESTIGATION AND RESOLUTION PROCEDURE

28. **Complaints and Investigation**

(1) A payment service provider shall:

(a) Establish formalized procedures for the lodgment of complaints by customers of matters covered by this Directive;

(b) Establish appropriate procedures for the investigation and resolution of any complaint by a customer; and

(c) Set out in standard terms and conditions the means and procedures to lodge a complaint.

(2) A customer is required to disclose to the institution all relevant information relating to the complaint except his access code.

(3) The institution shall, as far as possible, settle all complaints immediately.

(4) The institution's decision in relation to a complaint is to be made on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence.

(5) Where an institution is unable to settle a complaint immediately as required under subsection (3), it shall inform the customer immediately for the need of 15 days to resolve the complaint.

(6) Where an institution is unable to resolve the complaint within 15 days, it shall notify the customer in writing of the need for an extension of time which shall not in any case exceed 30 days from the date the complaint is lodged.

(7) An institution shall promptly advise the customer of the outcome of the investigation, together with reasons for the outcome upon completion of its investigation.

29. **Incorrectly credited or debited account**

(1) Where as a result of the investigation of a complaint, an institution discovers that the customer's account has been incorrectly credited or debited, it where appropriate, shall:

(a) Make adjustment to the customer's account including interest or charges within 15 days from acknowledgment; and

(b) Notify the customer in writing of the adjustments made to his account.

30. **Institution to provide information**

(1) Where an institution is of the view that the customer is liable for loss arising from any loss, misuse, theft or unauthorized use of a card or breach of access code security:

(a) The institution is to make available to the customer, copies of any documents or other evidence relevant to the outcome of its investigation, including information from the log of transactions; and

(b) The institution is also to refer to the systems log to establish whether there was any system or equipment malfunction at the time of the transactions, and advise the customer in writing of the outcome of its inquiry.

(2) Provided always that the institution will not be required to furnish any information that has a direct relation to or impacts the security of the institution or its system.

31. **Information and advice on appeal**

(1) The complaint procedure shall contain information relating to:

(a) The right of a customer to appeal against the outcome of his complaint to the senior management; and

(b) The right of a customer to refer the complaint to the Central Bank, or any other body authorized by the Central Bank, if he is not satisfied with the outcome of his complaint.

(2) The institution shall make known or make available the information in subparagraph (1) to a customer.

32. **Records of complaint**

(1) An institution shall keep a record of complaints and their resolutions, so that aggregate data on the type, frequency and resolution of such complaints can be made available to the Central Bank or any other body authorized by it as and when required.

33. **Audit trails**

An institution shall ensure that their electronic fund transfers generate sufficient records to enable a transaction to be traced, checked and where any error has occurred, to be identified and corrected.

PART VII

MISCELLANEOUS

34. **Privacy**

(1) An institution shall ensure that all information relating to an electronic fund transfer of its customer shall not be disclosed unless permitted by a Central Bank Directive or other acts. This shall include reporting of fraudulent transactions to relevant operators and/or industry body as expressly recognized by the Central Bank.

(2) No person other than, an officer of or agent appointed by, the institution that maintains the account, or the customer, may have access to information relating to electronic fund transfer, the affairs or an account of the customer.

(3) No electronic terminal shall be capable of providing any information relating to an electronic fund transfer, the affairs or an account of a customer unless:

(a) The electronic fund transfer is operated by an authorized officer or agent appointed by the institution; or

(b) The request for information is preceded by the entry of the correct customer's access code or card number or equivalent.

(4) An institution shall not provide any information relating to an electronic fund transfer, the affairs or an account of a customer unless the information is provided:

(a) Pursuant to a legal duty or responsibility; or

(b) With the consent of a customer.

(5) The rules governing the operation of individual accounts will be applicable to electronic fund transfers in relation to disclosure of information to third parties.

35. **Waiver of rights and greater protection**

(1) No agreement in writing between a customer and a bank or other payment service provider may contain any provision that constitutes a waiver of any right conferred or cause of action created by this Directive.

(2) Nothing in this Directive shall prohibit any agreement, which grants a customer more extensive rights, or remedies or greater protection than those contained in this Directive.

36. **Special regime or derogation**

The Central Bank may issue special regimes or derogation for specific categories of payment services or instruments in relation to their structure, costs and efficiency of measures to protect the users.