South African Reserve Bank

National Payment System Department

Draft for consultation

Directive in respect of specified payment activities within the national payment system

Directive X of 2026

May 2026

Contents

Part 1: Background, structure, definitions, application and scope

1. Background

1.1 In terms of section 10(1)(c) of the South African Reserve Bank Act, 1989 (Act No. 90 of 1989), as amended, the South African Reserve Bank (Reserve Bank) is required to perform such functions, implement such rules and procedures, and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems. Furthermore, the National Payment System Act, 1998 (Act No. 78 of 1998), as amended (NPS Act), provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in the Republic of South Africa (RSA), and for connected matters.

1.2 The national payment system (NPS) encompasses the entire payment process, from payer to beneficiary, and includes settlement between banks. The process includes all the tools, systems, instruments, mechanisms, institutions, agreements, procedures, rules or laws applied or utilised to effect payment. The NPS is a primary component of the country's monetary and financial system as it enables the circulation of money and assists transacting parties to make payments and exchange value.

1.3 In terms of section 12(1) of the NPS Act, the Reserve Bank may, from time to time, and after consultation with the payment system management body (PSMB), issue directives to any person regarding a payment system or the application of the provisions of the NPS Act. The considerations for issuing a directive take account of the integrity, effectiveness, efficiency and security of the NPS and national financial stability as well as any other matters that the Reserve Bank considers appropriate.

1.4 Payment activities are vital for the safe and efficient functioning of the economy. Robust authorisation requirements are therefore critical, and generally more extensive for inner core activities such as payment account services, clearing and settlement, which demand a higher level of regulatory scrutiny. Applicants are expected to submit well-prepared applications that demonstrate their capacity to meet the applicable requirements set out in this Directive.

1.5 This Directive sets forth the requirements that any person (whether a bank or non-bank) must meet to offer or conduct specified payment activities as detailed in Annexure B, as well as those provided within closed-loop payment systems. The activities specified in Annexure B include both those exempted from the definition of 'the business of a bank' under the Banks Act, 1990 (Act No. 94 of 1990), as amended, pursuant to Notice XX of 2026 (Exemption Notice), as well as those not exempted by the Exemption Notice. Additionally, the further purpose and objectives of this Directive are described in paragraph 5.

2. Structure of the Directive

2.1 Part 1: Background, structure, definitions, application and scope

2.2 Part 2: Purpose, position, exemptions and sponsorships

2.3 Part 3: Application to conduct a payment activity in Annexure B

2.4 Part 4: Closed-loop payment system and payment activities

2.5 Part 5: Reserve Bank powers and responsibilities

2.6 Part 6: Annexures

3. Definitions

In this Directive, unless the context indicates otherwise, the words and expressions used shall have the same meaning as assigned to them in the NPS Act, and similar expressions shall have corresponding meanings.

3.1 **'Acquiring of payment instructions'** means a payment activity provided by a payment institution to a payee or a payer to accept and process payment instructions, which results in a transfer of funds to the payee, irrespective of the payment instrument used by the payer.

3.2 **‘Agent’** means a third party who acts on behalf of a payment institution under an agency agreement to conduct payment activities.

3.3 **‘Agency agreement’** is a written contractual agreement between:

a. a payment institution and an agent;

b. a master agent and an agent; or

c. a payment institution and master agent.

3.4 **‘Agency business’** means the provision of payment activities by an agent to clients of a payment institution on behalf of the payment institution.

3.5 **‘Agent point’** means a physical or digital location within the RSA where agency business is provided.

3.6 **‘Authorisation’** means the Reserve Bank granting permission for a payment institution to conduct a payment activity listed in Annexure B.

3.7 **‘Banks Act’** means the Banks Act, 1990 (Act No. 94 of 1990), as amended.

3.8 **‘Beneficial owner’** means a beneficial owner as defined in the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), as amended.

3.9 **‘Beneficiary service provider’** means a juristic person who accepts money or the proceeds of payment instructions from multiple payers on behalf of a beneficiary as a regular feature of that person’s business.

3.10 **‘Business day’** means any day other than a Saturday, Sunday or public holiday in the RSA.

3.11 **‘Clearing’** means ‘clearing’ as defined in the NPS Act.

3.12 **‘Clearing system participant'** means a participant as defined in the NPS Act.

3.13 **‘Client’** means a natural or juristic person to whom or for whom a payment activity

is performed/conducted or with whom a payment institution has a relationship to conduct a payment activity, in whatever capacity, and includes a successor in title of such person.

3.14 **'Client funds'** means any funds held, kept in safe custody, controlled, or administered on behalf of a client when conducting or providing payment activities listed in Annexure B, and safeguarded as outlined in paragraph 9 of Annexure A.

3.15 **'Client-consented data'** means client data collected, held and used by a payment institution, including client transactions, personal identification data and client financial history, which the client of the payment institution has, in accordance with the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPI Act), consented to be accessed by a third party.

3.16 **'Closed-loop payment system or closed-loop payment activity'** means a payment system or payment activity, including but not limited to the issuance of e-money, a payment instrument, or money remittance that is not interoperable and is provided or conducted by a single service provider for intended use within a limited network or ecosystem, and both the payer and the payee who are clients of the service provider participate in the same payment system or payment activity provided by the service provider.

3.17 **'Control function'** means each of the following:

a. a risk management function;
b. a compliance function; and
c. an internal audit function.

3.18 **'Credit payment instruction'** means a payment instruction from the payer to a payment account service provider, presented in the form of an electronic record, to transfer funds to a payee.

3.19 **'Crypto asset'** means for the purpose of this directive, a digital representation of value that is not issued by a central bank, but is capable of being transferred or stored electronically by natural and legal persons for the purpose of payment, applies cryptographic techniques and/or uses distributed ledger technology.

3.20 **'Designated clearing system participant'** means a person specified in the notice referred to in section 6(3)(a) of the NPS Act;

3.21 **'Designated settlement system'** means a settlement system designated in terms of section 4A of the NPS Act.

3.22 **'Designated settlement system operator'** means a 'designated settlement system operator' as defined in the NPS Act.

3.23 **'Digital location'** means a virtual point within the RSA where agency business is conducted through electronic channels, such as online platforms or mobile applications, enabling customers to access payment activities without a physical presence.

3.24 **'Due diligence'** means:

a. the duty of payment institutions that are accountable institutions to conduct customer due diligence to identify and verify clients as set out in sections 20A-21H of the FIC Act; or
b. the duty of payment institutions that are not accountable institutions to identify and verify clients as set out in Annexure K of this Directive.

3.25 **'Exemption Notice'** means Notice XX of 2026 issued in terms of paragraph (cc) of the definition of 'the business of a bank' in section 1(1) of the Banks Act.

3.26 **'E-money'** means a store-of-value product that (i) is a digital representation of a fiat currency (legal tender); (ii) is a claim against the e-money issuer; and (iii) may be redeemed for money or by transfer into a payment account at face value on demand. E-money is held for payment purposes and may be accepted as a means of payment by persons other than the issuer in an open-loop payment system or be accepted within the issuer's network or ecosystem in the closed-loop payment system. For the purposes of this Directive, e-money includes 'mobile money', is also referred to as Payment Account C and excludes Payment Account A,

Payment Account B, crypto assets and tokenised assets.

3.27 **'E-money issuer'** means an entity that issues e-money.

3.28 **'Face value'** means the e-money amount equivalent to the ZAR value.

3.29 **'FIC Act'** means the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001), as amended.

3.30 **'FSR Act'** means the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017), as amended.

3.31 **'Funds'** means a monetary claim on a party acceptable to the payee in the form of cash, a balance or credit to a payment account, or credit to an account held in the books of the Reserve Bank settlement system or designated settlement system.

3.32 **'Governing body'** in relation to a payment institution means a person or body of persons, whether elected or not, that manages, controls, formulates the policy and strategy of the payment institution, directs its affairs or has the authority to exercise the powers and perform the functions of the payment institution.

3.33 **'Informed consent'** means any voluntary, specific and informed expression of will in terms of which consent is given by the payer for processing the payer's information, including personalised credentials, for purposes of payment initiation.

3.34 **'Interface infrastructure'** means a system or an application that enables payment account service providers and payment initiation service providers to interact with each other and payer, to exchange information in respect of payment instructions.

3.35 **'Interoperable'** means the technical or legal compatibility that enables a system or mechanism to operate seamlessly and is to be used in conjunction with other systems or mechanisms. Interoperability allows participants within payment systems to clear and settle payment instructions within or between payment systems without the need to participate in multiple systems.

3.36 **'Issuance of payment instruments'** means the provision to payer or payee of

payment instruments, excluding Payment Account A and Payment Account B, in a closed-loop payment system or open-loop payment system that allows a payer or payee to make a payment or transfer funds or receive funds.

3.37 **'Key person'** in relation to a payment institution means each of the following persons:

a. a member of the governing body of the payment institution;
b. the chief executive officer or other person performing executive duties within the payment institution;
c. a person other than a member of the governing body of the payment institution who makes or participates in making decisions that:
    i. affect the whole or a substantial part of the business of the payment institution; or
    ii. have the capacity to affect significantly the financial standing of the payment institution;
d. a person other than a member of the governing body of the payment institution who oversees the enforcement of policies and/or the implementation of strategies approved or adopted by the governing body of the payment institution;
e. the head of a control function of the payment institution; or
f. the head of a function of the payment institution that this Directive requires to be performed.

3.38 **'Master agent'** means a person who has an agency agreement with a payment institution to contract and manage agents that provide agency business.

3.39 **'Mobile money'** means a form of e-money provided through a store of value that enables users to store, send and receive funds using a mobile device or mobile network.

3.40 **'Money remittance'** means a service for the transmission of funds within South Africa, with or without any payment accounts being created in the name of the payer or the payee, where:

a. funds are received from a payer for the sole purpose of transferring a

corresponding amount to a payee or to another payment institution acting on behalf of the payee; or

b. funds are received on behalf of, and made available to, the payee.

The categories of money remittances include the following subcategories:

i. funds-in, funds-out service based on a contractual relationship between the money remitter and the payer; and

ii. funds-in, funds-out service involving a single instruction or transaction.

3.41 **'Open-loop payment system'** means a payment system that is operated by multiple payment institutions that provide interoperable payment methods and services, or payment activities referred to under Annexure B allowing end users to make payments to any payee.

3.42 **'Operator of a closed-loop payment system'** means a person that operates a closed-loop payment system.

3.43 **'Outsourcing arrangement'** means an arrangement between a payment institution and another person for the provision of, or for the payment institution to carry out, any of the following:

a. a control function;

b. a function that is integral to the nature of a payment activity that the payment institution provides, excluding:

i. a contract of employment between the payment institution and a staff member; or

ii. an arrangement between a payment institution and a person for the person to act as an agent of the payment institution to provide a payment activity, including an agency business or agency agreement.

3.44 **'Payee'** means a natural or juristic person who is the recipient of funds which have been the subject of a payment instruction.

3.45 **'Payer'** means a natural or juristic person who holds a payment account and allows a payment instruction in respect of funds from that payment account, or where

there is no payment account, a natural or juristic person who gives a payment instruction regarding its own funds.

3.46 **'Payer service provider'** means a juristic person that accepts money or proceeds of payment instructions from a payer to make payment on behalf of that payer to multiple beneficiaries as a regular feature of that person's business.

3.47 **'Payment'** means the transfer of funds from a payer to a payee.

3.48 **'Payment account'** means an account or store of value that is used for the transfer of funds, and includes:

a. Payment Account A (Group G in Annexure B);
b. Payment Account B (Group G in Annexure B); or
c. Payment Account C (Group A1 in Annexure B).

3.49 **'Payment Account A'** means an account provided by an entity that accepts deposits as defined in section 1(1) of the Banks Act.

3.50 **'Payment Account B'** means an account provided by an entity that provides credit or credit facility as defined in section 1 of the National Credit Act, 2005 (Act No. 4 of 2005), as amended.

3.51 **'Payment Account C'** is an e-money account that is distinct from a bank account or provision of credit or credit facility.

3.52 **'Payment account service provider'** means a payment institution that provides and maintains a payment account for a payer or payee.

3.53 **'Payment activity'** means an activity listed in Annexure B.

3.54 **'Payment clearing house (PCH)'** means an arrangement between two or more clearing system participants and Reserve Bank settlement system participants, excluding a designated settlement system operator, governing the clearing or netting of payment instructions between those clearing system participants and Reserve Bank settlement system participants, as defined in section 1 of the NPS Act.

3.55 **'Payment execution'** means the ability of a payment institution to submit clearing

and/or settlement instructions or to process payment instructions for the purposes of clearing or settlement.

3.56 **'Payment initiation'** means an electronic service to initiate a credit payment instruction by a payment initiation service provider at the request of the payer with respect to a payment account held at a payment account service provider.

3.57 **'Payment initiation service provider'** means a person that is authorised to provide payment initiation.

3.58 **'Payment institution'** means a person authorised and/or designated as a clearing system participant and/or exempted, where applicable, in terms of the NPS Act and this Directive to perform a payment activity listed in the Exemption Notice and/or Annexure B.

3.59 **'Payment instruction'** means an instruction as defined in the NPS Act.

3.60 **'Payment instrument'** means a physical or electronic tool or mechanism, which is used to initiate a payment instruction enabling the transfer of funds from a payer to a payee.

3.61 **'Payment system'** means a 'payment system' as defined in the NPS Act and includes a closed-loop payment system or an open-loop payment system.

3.62 **'PCH system operator'** means a 'PCH system operator' as defined in the NPS Act.

3.63 **'Personalised security credentials'** means personalised features provided by the payment institution to a payer for the purposes of authentication.

3.64 **'POCA'** means the Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998).

3.65 **'POCDATARA'** means the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

3.66 **'POPI Act'** means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

3.67 **‘Redeemable for cash’** means the value represented by a payment instrument, e-money, or a store of value that may be exchanged for ZAR or credited to a payment account upon demand by the holder.

3.68 **‘Redemption/redeem’** means the withdrawal of funds or the electronic transfer of the equivalent value in ZAR from the e-money issuer to the e-money client, upon the e-money client’s request. Redemption is strictly limited to the return of ZAR to the e-money client and does not include the purchase of goods or services, nor the onward transfer of value to another beneficiary or store of value.

3.69 **‘Registration’** means the granting of permission by the Reserve Bank to a person to conduct a closed-loop payment system or payment activity, or to a payment institution to sponsor another person to conduct a closed-loop payment system or payment activity.

3.70 **‘Registered person’** means a person registered in terms of the regulatory framework to operate a closed-loop payment system or conduct a closed-loop payment activity.

3.71 **‘Reserve Bank settlement system’** means the ‘Reserve Bank settlement system’ as defined in the NPS Act.

3.72 **‘RSA’** means the Republic of South Africa.

3.73 **‘Scheduled payment instruction’** means a payment instruction that is scheduled by the payer for a specific date whether agreed or not between the payer and the payee.

3.74 **‘Scheme’** means a set of formal, standardised and common binding rules governing the relationship between payment institutions or an agreed-upon arrangement between payment institutions defining the functional, business, legal and technical rules for executing payments using a particular payment instrument.

3.75 **‘Scheme manager’** means the legal entity or body responsible for the overall governance, rule-setting and management of a scheme, including the establishment, maintenance and enforcement of the scheme’s rules, membership

criteria and compliance framework.

3.76 ‘**Security incident’** means an event that adversely affects the security of an information system and/or the information that the system processes, stores or transmits, or which violates the security policies, security procedures and/or acceptable use policies of the payment institution, whether resulting from malicious activity or not.

3.77 **‘Segregated account’** means a formal beneficiary account as defined in the Deposit Insurance Regulations issued in terms of the Financial Sector Regulation Act, 2017 (Act No. 9 of 2017) held at a bank, or a settlement account of a designated settlement system participant held in a designated settlement system.

3.78 **‘Sensitive payment data’** means data, including personalised security credentials, which can be used to initiate fraudulent payment instructions or gain control of the payer’s payment account. For the activities of payment initiation service providers, the name of the account owner and the account number do not constitute sensitive payment data.

3.79 **‘Settlement’** means ‘settlement’ as defined in the NPS Act.

3.80 **‘Settlement system’** means a ‘settlement system’ as defined in the NPS Act.

3.81 **‘Settlement system participant’** means a ‘settlement system participant’ as defined in the NPS Act.

3.82 **‘Sponsorship’** means the process by which an authorised, designated or registered payment institution provides indirect access to the NPS for another entity, including access for a closed-loop payment system as well as activities such as acquiring, clearing, settlement and payment to third persons**,** as contemplated in paragraph 8.

3.83 **‘Store of value’** means funds stored in a mechanism provided by a payment institution or within a closed loop payment system.

3.84 **‘Strong client authentication’** means an authentication based on the use of two or more elements categorised as knowledge (something only the payer knows),

possession (something only the payer possesses) and inherence (something the payer is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

3.85 **'System operator'** means a 'system operator' as defined in the NPS Act.

3.86 **'Third-party payment'** means the acceptance of money or payment instructions by third-party payment providers as a regular feature of business from any other person, for the purpose of making payment on behalf of that other person to a third party to whom that payment is due, as contemplated in section 7 of the NPS Act.

3.87 **'Third-party payment provider' (TPPP)** means a juristic person that provides third-party payment services. A TPPP may be a payer service provider and/or a beneficiary service provider as defined in 3.46 and 3.9 above respectively.

3.88 **'Tokenised asset'** means a digital representation of a traditional asset on a programmable platform.

3.89 **'Variation'** means amending, deleting, replacing or varying authorisation conditions or imposing other or additional conditions and/or amending the payment activities or subcategories of payment activities that the payment institution is authorised or designated to undertake, or varying sponsorship arrangements or the exemption of a payment institution, including variation as contemplated in the NPS Act.

4. Application and scope of this Directive

4.1 This Directive applies to all persons conducting or applying to conduct payment activities listed in Annexure B and closed-loop payment systems or payment activities respectively, except where otherwise stated, specifically excluded or exempted.

4.2 This Directive is applicable to domestic payments activities listed in Annexure B and closed-loop payment systems and payment activities outlined in Part 4 of this Directive.

4.3 The following are excluded from the scope of this Directive:

4.3.1 authorisation of system operators, which is provided for under a separate regulatory framework;

4.3.2 authorisation of payment clearing house (PCH) system operators which is provided under a separate regulatory framework;

4.3.3 authorisation to provide Payment Account A and Payment Account B, as outlined in Annexure B, Group G. These authorisations remain the responsibility of the Prudential Authority in terms of the Banks Act and National Credit Regulator in terms of the National Credit Act, although certain specified requirements of this Directive apply where these accounts are used to transfer funds, or make or receive a payment;

4.3.4 cross-border payment activities and closed-loop payment systems and activities; and

4.3.5 designated settlement systems, in accordance with section 12(4) of the NPS Act.

4.4 System operators and PCH system operators are not required to comply with this Directive.

Part 2: Purpose, objective, position, exemptions and sponsorships

5. Purpose and objective

5.1. This Directive aims to promote competition, innovation and financial inclusion in the NPS. With technological advancements, non-banks are increasingly participating in the payment ecosystem. Non-banks were previously prohibited from holding client funds in the absence of a sponsorship arrangement with a licensed bank or being a registered third-party payment provider (TPPP). This Directive provides for an activity-based regulatory framework that allows direct access to the NPS and enables any juristic person, both banks and non-banks, to offer payment activities listed in Annexure B and/or closed-loop payment systems or payment activities, if they meet the applicable authorisation or registration requirements.

5.2. This Directive outlines the following:

5.2.1 authorisation and designation requirements to conduct payment activities listed in Annexure B;

5.2.2 ongoing compliance requirements with the Directive by payment institutions;

5.2.3 registration of closed-loop payment system and payment activities;

5.2.4 requirements for the Reserve Bank settlement system operator;

5.2.5 requirements for payment account service providers in respect of a payment initiation activity contained in Annexure B;

5.2.6 the powers and responsibilities of the Reserve Bank; and

5.2.7 transitional arrangements for payment activities.

6. Position of the Reserve Bank

6.1 The Reserve Bank supports innovative and interoperable payment activities that improve the efficiency, accessibility, safety and integrity of the NPS and enhance the safety and soundness of the payment institutions.

6.2 A payment activity and closed-loop payment system or payment activity listed or referred to in the Exemption Notice, which is performed by a payment institution

that is not a bank, is exempt from the definition of 'the business of a bank' as outlined in the Banks Act.

6.3 Any person that provides a payment activity listed in Annexure B must obtain authorisation or designation from the Reserve Bank to offer the payment activity in accordance with this Directive. In respect of payment activities requiring clearing and settlement, the applicant must comply with paragraphs 18 to 20.

6.4 Any person that provides a closed-loop payment system or payment activity listed in paragraph 42.4 must obtain registration from the Reserve Bank to offer the payment activity in accordance with this Directive.

6.5 If a person seeks to apply to conduct more than one payment activity, a single application must be submitted demonstrating that the person meets all the requirements applicable for each payment activity. Where a person is already authorised or designated and seeks to add a payment activity, a new application must be submitted. This application should confirm whether the previously submitted information relating to the pre-existing authorisation or designation remains applicable and provide any updated documentation or information where necessary, including all required information and supporting documents relevant to the additional payment activity.

6.6 Any payment activity and closed-loop payment system or payment activity involving acceptance of deposits or the solicitation or advertising of deposits as defined in the Banks Act that is not listed in the Exemption Notice will continue to be regarded as 'the business of a bank' and remain subject to the Banks Act. Therefore, non-banks conducting these activities must either obtain a banking license or be sponsored by a bank. Any non-bank offering such payment activities or closed-loop payment systems or activities without being registered as a bank or sponsored by a bank will be contravening the Banks Act.

6.7 The Reserve Bank retains the discretion to decline, with reasons, any application for designation under the NPS Act, and authorisation registration that fails to comply with the requirements stipulated in this Directive**.** Applicants whose applications have been declined may submit a new application no earlier than thirty (30) days following the date of the decline notification, provided that the

subsequent application fully addresses the shortcomings of the initial application and complies with all applicable requirements.

6.8 Interoperable payment transactions must comply with the applicable scheme rules as well as the clearing and settlement requirements and timelines outlined in the NPS Act and related directives, including this Directive. This includes compliance with relevant PCH agreements between participants and between participants and PCH system operators, settlement agreements, scheme agreements as well as the rules and operational procedures for schemes, clearing and settlement.

6.9 The Reserve Bank will publish an updated list of authorised and designated payment institutions as well as registered closed-loop payment systems on its website, which will be updated regularly.

7. Exemptions

7.1 The Reserve Bank may, upon application or at its own discretion, exempt any person conducting a payment activity, or a closed-loop payment system or payment activity from complying with any part of this Directive, where:

7.1.1 practicalities impede the application of a part, provision or requirement of this Directive;

7.1.2 where such person conducts an activity similar to a payment activity regulated under this Directive, under existing legislation;

7.1.3 any existing legislation also regulates a payment activity; or

7.1.4 it is consistent with the achievement of the following NPS objectives:

a. the stability, safety, efficiency, transparency and integrity of the NPS;
b. the safety and soundness of payment institutions;
c. confidence in the NPS;
d. financial inclusion, competition and innovation in the NPS; or
e. the public interest.

7.2 The Reserve Bank may grant an exemption to different categories, subcategories, types or kinds of applicants or payment institutions from the provisions of this Directive. However, the Reserve Bank may not grant an exemption from payment activities or conditions contemplated in the Exemption Notice.

7.3 An exemption granted under paragraph 7 of this Directive may be provided for a specified period and subject to conditions as prescribed by the Reserve Bank.

7.4 The Reserve Bank may deny an exemption from this Directive if it could lead to a systemic event as defined in the FSR Act or pose a risk to the safety and efficiency of the NPS, including the safety and soundness of payment institutions and safeguarding of client funds.

7.5 An exemption may be withdrawn or suspended in its entirety or in part on any grounds which the Reserve Bank, may consider justifiable, including but not limited to non-compliance with the stipulated conditions. The Reserve Bank, will provide written reasons for the withdrawal or suspension to the payment institution.

7.6 The Reserve Bank may publish an exemption on its website, with reasons for granting the exemption.

7.7 Persons registered as banks by the Prudential Authority under the Banks Act are exempt from providing the authorisation information/supporting documentation relating to the following requirements, provided that the information and documentation have been provided to the Prudential Authority, and such person is subject to the regulation and supervision of the Prudential Authority under the Banks Act:

7.7.1 general application requirements: paragraph 2 of Annexure A;
7.7.2 organisational structure: paragraph 3 of Annexure A;
7.7.3 governance arrangements: paragraph 4 of Annexure A;
7.7.4 fit-and-proper requirements: paragraph 6 of Annexure A;
7.7.5 prudential requirements: Annexure D;
7.7.6 safeguarding client funds: paragraph 9 of Annexure A, except the safeguarding of e-money;
7.7.7 prohibitions and restrictions: paragraph 13 of Annexure A; except the prohibitions and restrictions applicable to the issuance of e-money;
7.7.8 agency arrangements: paragraph 15 of Annexure A; and
7.7.9 outsourcing arrangements: paragraph 16 of Annexure A.

7.8 Persons registered as banks under the Banks Act must comply with reporting, risk

management controls, data protection, accounting and audit, value date and availability of funds, and client complaints requirements and ongoing requirements stipulated in this Directive relating to a payment activity and requirements relating to closed-loop payment systems and payment activities offered/conducted by a bank.

7.9 Where the Reserve Bank conducts or intends to conduct payment activities listed in Annexure B, it is/shall be exempt from complying with the following requirements of this Directive: organisational structure; governance arrangements requirements; fit-and-proper requirements; prudential requirements; and accounting requirement.

7.10 Persons permitted to provide a TPPP payment activity in terms of section 7 (a) and (b) of the NPS Act are exempted from authorisation in terms of this Directive; however, they are required to comply with requirements applicable to TPPPs.

8. Sponsorships

8.1 The Reserve Bank may, in its discretion, approve sponsorship on application, subject to the following sponsorship arrangements:

Closed-loop payment systems

8.1.1 A person that conducts or seeks to conduct payment activities within a closed-loop payment system, and whose transaction values fall below the prescribed threshold outlined in paragraph 42.8, may operate under a sponsorship arrangement with an authorised, or designated payment institution or registered person, or obtain registration in accordance with Part 4 of this Directive. The sponsoring payment institution must be duly authorised or designated to conduct the payment activity under Annexure B and meet the sponsorship requirements as may be prescribed by the Reserve Bank.

8.1.2 The sponsoring payment institution must ensure its compliance and that the sponsored institution complies with the registration and ongoing requirements outlined in paragraph 42.5 to 43 respectively, including any requirements prescribed by the Reserve Bank.

8.1.3 The Reserve Bank may, in its discretion, vary, suspend or revoke, on any justifiable

grounds and with reasons, its approval of a sponsorship arrangement granted in terms of paragraph 8.1 above.

Clearing

8.1.4 Where a payment institution that conducts interoperable payment activities does not meet the Reserve Bank designation requirements as provided for in section 6(3) of the NPS Act, scheme membership requirements or the PCH system operator's eligibility and participation criteria, does not conclude the PCH system operator agreements or does not wish to apply for authorisation as a clearing system participant or designated clearing system participant (DCSP), such a payment institution must appoint a clearing system participant or a DCSP to clear payment instructions on its behalf, provided the clearing system participant or DCSP meets the sponsorship requirements to be prescribed by the Reserve Bank.

8.1.5 The sponsoring payment institution must be authorised or designated as a clearing system participant in terms of this Directive and the NPS Act.

8.1.6 A sponsoring payment institution is accountable and liable for the clearing risks associated with the sponsored payment institution.

8.1.7 The sponsoring payment institution and sponsored payment institution must jointly provide prior written notice to the Reserve Bank of the sponsorship arrangement, demonstrating compliance with the sponsorship requirements prescribed by the Reserve Bank, and confirming that the sponsoring payment institution will clear payment instructions on behalf of the sponsored payment institution.

Settlement

8.1.8 Where a payment institution that conducts interoperable payment activities does not meet the criteria for settlement system participants required by the NPS Act, the settlement system operator's eligibility and participation criteria, does not conclude the settlement system operator agreements or does not wish to apply to be authorised as a settlement system participant, it must appoint a Reserve bank settlement system participant or a designated settlement system participant to

settle payment obligations on its behalf, provided the Reserve Bank settlement system participant or designated settlement system participant meets the sponsorship requirements prescribed by the Reserve Bank.

8.1.9 The sponsoring payment institution must be authorised or designated as a Reserve Bank settlement system participant or designated settlement system participant in terms of this Directive and the NPS Act.

8.1.10 A sponsoring payment institution is accountable and liable for the settlement risks associated with the sponsored payment institution.

8.1.11 A sponsored payment institution must submit a signed letter from the sponsoring payment institution that it is a Reserve Bank settlement system participant or designated settlement system participant, demonstrating that it meets the sponsorship requirements of the Reserve Bank and confirm that it will settle the payment obligations on behalf of the sponsored payment institution.

Acquiring

8.1.12 A person who seeks to conduct an acquiring payment activity through sponsorship may operate under a sponsorship arrangement with a sponsoring payment institution. The sponsoring payment institution must be duly authorised to conduct the acquiring payment activity and meet the sponsorship requirements as may be prescribed by the Reserve Bank.

8.1.13 A sponsoring payment institution is accountable and liable, within reason, for its approval of a sponsorship arrangement granted in terms of paragraph 8.1 above.

Third-party payment provider

8.1.14 A payment institution that conducts or seeks to conduct a TPPP business activity as provided for in Group D under sections 24 to 34, may operate under a sponsorship arrangement with any sponsoring payment institutions outlined in sections 7(a) and (b) of the NPS Act, and another authorised TPPP that meets the sponsorship requirements as may be prescribed by the Reserve Bank.

8.1.15 The sponsoring payment institution must ensure that it complies with its own obligations in terms of this Directive and that the sponsored institution complies with the applicable requirements in Group D under sections 24 to 34, including any other requirements prescribed by the Reserve Bank.

8.1.16 A sponsoring payment institution is accountable and liable for the TPPP business activity risks associated with the sponsored TPPP.

8.1.17 The Reserve Bank may, in its discretion, vary, suspend or revoke, on any justifiable grounds, its approval of a sponsorship arrangement granted in terms of paragraph 8.1 above.

Part 3: Application to conduct a payment activity in Annexure B

Group A: Issuing of e-money or payment instruments

Category A1: Issuing of e-money

9. Authorisation requirements for Tier 1 e-money issuer

9.1 A person who seeks to issue e-money on a large scale of R5 million and more in average monthly e-money liabilities over a period of six (6) consecutive months, must issue e-money in an interoperable payment system, apply to the Reserve Bank for authorisation as a Tier 1 e-money issuer and participate in the domestic faster payments system.

9.2 An application under paragraph 9.1 must be submitted in a form as set out in Annexure C accompanied by the information prescribed therein.

9.3 A person who seeks authorisation as Tier 1 e-money issuer must meet the application requirements in paragraphs 2 to 4, 6 to 8 and 17 of Annexure A.

9.4 In addition to the general requirements, a person who seeks authorisation as a Tier 1 e-money issuer must meet the following requirements:

9.4.1 enter into an agreement with every client for whom it opens an e-money account;

9.4.2 exchange funds received for e-money;

9.4.3 issue e-money at face value on the receipt of funds that may be redeemed for money or by transfer into a payment account at face value on demand;

9.4.4 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in Annexure D;

9.4.5 open and maintain a segregated account to safeguard the client funds as set out in paragraph 9 of Annexure A, and provide evidence of such an account at the time of application;

9.4.6 establish systems to maintain accurate and complete records of e-money accounts opened, the identity of e-money clients, transactions undertaken by clients and the individual and aggregate balances held by clients;

9.4.7 does not issue e-money accounts with a transaction limit that exceeds:

a. per individual – for natural persons: R15 000 per day and R50 000 per month or as may be amended by the Reserve Bank from time to time; and
b. for juristic persons: R250 000 per month per entity or as may be amended by the Reserve Bank from time to time;

9.4.8 must not have a maximum balance limit on individual e-money accounts which exceeds:

a. natural person: R50 000 or as may be amended by the Reserve Bank from time to time; and
b. juristic person: R100 000 per entity or as may be amended by the Reserve Bank from time to time; and

9.4.9 indicate the type of payment activities that will be conducted or payment instruments to be issued using e-money.

9.5 Where an e-money client has more than one e-money account with a particular e-money issuer, that e-money issuer must ensure that the total balance across all accounts does not exceed the limits specified in paragraphs 9.4.7 and 9.4.8 above.

9.6 A Tier 1 e-money issuer must:

9.6.1 where a Tier 1 e-money issuer is a non-bank, be designated as a clearing system participant by the Reserve Bank, or where a Tier-1 e-money issuer is a bank, be authorised as a clearing system participant in terms of the NPS Act and this Directive or appoint a clearing system participant or DCSP to clear on its behalf subject to compliance with the sponsorship requirements as set out in paragraph 8;

9.6.2 where the Tier 1 e-money issuer is either a bank or non-bank, be authorised as a member of a PSMB or scheme and participate in the relevant PCHs or scheme or appoint an authorised PSMB or scheme member to participate in the relevant PCH or scheme on its behalf;

9.6.3 meet the entry and participation requirements for settlement system participants as set out in this Directive, and by the Reserve Bank settlement system operator

as approved by the Reserve Bank, to settle payment obligations linked to its payment activity, or appoint a Reserve Bank settlement system participant to settle payment obligations on its behalf in accordance with section 4(2)(d) of the NPS Act subject to compliance with sponsorship requirements under paragraph 8, if settlement is in the Reserve Bank settlement system, or be designated as a settlement system participant or appoint a designated settlement system participant to settle payment obligations on its behalf subject to compliance with sponsorship requirements under paragraph 8;

9.6.4 unless sponsored, comply with the clearing and settlement requirements and timelines duly aligned to the clearing and settlement requirements as provided for in the NPS Act and directives, PCH agreements, settlement agreements, clearing and settlement rules, clearing and settlement operational procedures or relevant instrument(s) issued by the Reserve Bank, PSMB or scheme manager, the PCH system operators and operators of settlement systems and designated settlement systems, as the case may be; and

9.6.5 register with the Financial Intelligence Centre (FIC) as an accountable institution under item 19 and item 23 of Schedule 1 of the Financial Intelligence Centre Act, 38 of 2001, as amended (FIC Act), within thirty (30) business days of issuance of the authorisation.

9.7 A Tier 1 e-money issuer is to commence with the activity of e-money issuing within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank, failing which the authorisation would be automatically revoked.

10. Ongoing requirements for Tier 1 e-money issuer

10.1 A Tier 1 e-money issuer must comply with the following requirements on an ongoing basis:

10.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

10.1.2 comply with the requirements in paragraphs 5 to 14 of Annexure A;

10.1.3 comply with the requirements in Annexure H;

10.1.4 comply with the anti-money laundering, counter terrorism financing and counter proliferation (AML/CFT/CPF) requirements in Annexure K;

10.1.5 where a Tier 1 e-money issuer appoints an agent or enters into outsourcing arrangements, comply with paragraphs 15 and 16 of Annexure A and provide information to the Reserve Bank as per Annexure F; and

10.1.6 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

11. Authorisation requirements for Tier 2 e-money issuer

11.1 A person who seeks to issue e-money on a limited scale with average monthly e-money liabilities below R5 million over a period of six (6) consecutive months in the interoperable payment system must apply to the Reserve Bank for authorisation as a Tier 2 e-money issuer and participate in a domestic faster payments system.

11.2 An application under paragraph 11.1 must be submitted in the form as set out in the Annexure C accompanied by information prescribed therein.

11.3 A person who seeks authorisation as Tier 2 e-money issuer must meet the application requirements in paragraphs 2 to 4, 6 to 8 and 17 of Annexure A.

11.4 A Tier 2 e-money issuer is exempted from complying with paragraphs 2.2.2, of Annexure A.

11.5 In addition to the general requirements, a person who seeks authorisation as Tier 2 e-money issuer must meet the following requirements:

11.5.1 exchange funds received for e-money;

11.5.2 must not issue e-money accounts with an individual transaction limit that exceeds R5 000 per day and R20 000 per month for natural persons and R100 000 per month for juristic persons, as may be amended by the Reserve Bank from time to time;

11.5.3 must not have a maximum e-money balance on e-money account which exceeds

R20 000 per natural or R50 000 for juristic persons;

11.5.4 indicate the type of payment activities that will be conducted or payment instruments to be issued using e-money;

11.5.5 ensure that, where an e-money client has more than one e-money account with a particular e-money issuer, the total balance across all accounts does not exceed the limits specified in paragraph 11.5.3;

11.5.6 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in the Annexure D; and

11.5.7 open and maintain a segregated bank account, safeguard the client funds as set out in paragraph 9 of Annexure A, and provide evidence of such an account on application.

11.6 A Tier 2 e-money issuer must:

11.6.1 where a Tier 2 e-money issuer is a non-bank, be designated as a clearing system participant by the Reserve Bank, or, where a Tier-2 e-money issuer is a bank, be authorised as a clearing system participant in terms of the NPS Act and this Directive or appoint a clearing system participant or DCSP to clear on its behalf subject to compliance with the sponsorship requirements as set out in paragraph 8;

11.6.2 where the Tier 2 e-money issuer is either a bank or non-bank, be authorised as a member of a PSMB or scheme and participate in the relevant PCHs or scheme or appoint an authorised PSMB member to participate in the relevant PCH or scheme on its behalf;

11.6.3 meet the entry and participation requirements for settlement system participants as set out in this Directive, and by the Reserve Bank settlement system operator as approved by the Reserve Bank, to settle payment obligations linked to its payment activity, or appoint a Reserve Bank settlement system participant to settle payment obligations on its behalf in accordance with section 4(2)(d) of the NPS Act subject to compliance with sponsorship requirements under paragraph 8, if

settlement is in the Reserve Bank settlement system, or be designated as a settlement system participant or appoint a designated settlement system participant to settle payment obligations on its behalf subject to compliance with sponsorship requirements under paragraph 8; and

11.6.4 unless sponsored, comply with the clearing and settlement requirements and timelines duly aligned to the clearing and settlement requirements as provided for in the NPS Act and directives, PCH agreements, settlement agreements, clearing and settlement rules, clearing and settlement operational procedures or relevant instrument(s) issued by the Reserve Bank, PSMB or scheme manager, the PCH system operators and operators of settlement systems and designated settlement systems, as the case may be.

11.6.5 register with the FIC as an accountable institution under item 19 and item 23 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

11.6.6 A Tier 2 e-money issuer is to commence with the activity of e-money issuing within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank, failing which the authorisation would be automatically revoked.

12. Ongoing requirements for Tier 2 e-money issuer

12.1 A Tier 2 e-money issuer must comply with the following requirements on an ongoing basis:

12.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

12.1.2 comply with the requirements under paragraphs 5 to 14 of Annexure A;

12.1.3 comply with the AML/CFT/CPF requirements in Annexure K;

12.1.4 where a Tier 2 e-money issuer appoints an agent or enters outsourcing arrangements, comply with paragraphs 15 and 16 of Annexure A, and provide information to the Reserve Bank as per Annexure F; and

12.1.5 inform and notify the Reserve Bank, in writing, of any amendments to the

information provided in their initial application within thirty (30) business days of the change.

13. Redemption of e-money for Tier 1 and Tier 2 e-money issuers

13.1 When redeeming the value of the e-money at the client's request, the e-money issuers must:

13.1.1 Ensure that the contract between the e-money issuer and e-money client clearly and prominently states the conditions of redemption, including any related fees or charges, and that the e-money client is informed of these conditions prior to agreeing to the contract or offer.

13.1.2 Subject redemption of the e-money to a fee only if stated in the contract and only in any of the following circumstances:

a. where redemption is requested prior to the termination of the contract; and

b. where the contract provides for a termination date and the e-money client terminates the contract prior to that date.

13.1.3 Where redemption is requested prior to the termination of the contract, allow the e-money client to request redemption of the e-money in whole or in part.

13.1.4 Where redemption is requested by the e-money client on or up to one year after the date of the termination of the contract:

a. the total monetary value of the e-money held must be redeemed; or

b. where the e-money issuer carries out one or more of the payment activities and it is unknown in advance what proportion of funds is to be used as e-money, all funds requested by the e-money client must be redeemed.

Category A2: Issuing of payment instruments

14. Authorisation requirements for issuing of a payment instrument

14.1 A person who seeks to issue a payment instrument that will be used or accepted in an interoperable payment system must apply to the Reserve Bank for authorisation to issue a payment instrument.

14.2 An application under paragraph 14.1 must be submitted in the form as set out in Annexure C accompanied by the information prescribed therein.

14.3 A person that seeks authorisation to issue payment instrument must meet the general requirements in paragraphs 2 to 4, 6 to 8, and 17 of Annexure A.

14.4 In addition to the general requirements, a person who seeks authorisation to issue payment instruments must meet the following requirements:

14.4.1 indicate to the Reserve Bank the specific type(s) of payment instrument(s) it intends to issue;

14.4.2 indicate to the Reserve Bank the types of payment accounts held by it and, where no payment accounts are held, the applicant is required to be authorised as a provider of payment accounts;

14.4.3 obtain membership in the PSMB or relevant scheme(s) and ensure full compliance with all PCH or scheme rules applicable to the specified type of payment instrument issued;

14.4.4 where the applicant is not already authorised or designated as a clearing system participant, unless sponsored, apply for and obtain such authorisation or designation in accordance with the authorisation or designation requirements to become a clearing system participant in paragraph 18;

14.4.5 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in the Annexure D; and

14.4.6 register with the FIC as an accountable institution under item 19 of Schedule 1 of

the FIC Act, within thirty (30) business days of issuance of the authorisation.

14.4.7 an issuer of a payment instrument must commence with the issuance of a payment instrument activity within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank, failing which the authorisation would be automatically revoked.

15. Ongoing requirements for issuing of a payment instrument

15.1 A person that issues payment instruments must, on an ongoing basis:

15.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

15.1.2 comply with paragraphs 5, 10, 11, 12, 13 and 14 of Annexure A;

15.1.3 ensure that the personalised security credentials are not accessible to persons other than the client to whom the payment instrument has been issued;

15.1.4 not send an unsolicited payment instrument, except where a payment instrument already issued to a client is to be replaced due to loss, damage, compromise, security or technical upgrades, expiry of the payment instrument; or new issuance relates to the provision of advanced services or enhanced features;

15.1.5 ensure that clients are informed of processes and contact details to notify the payment institution regarding the loss, theft, misappropriation or unauthorised use of the payment instrument;

15.1.6 on request, provide the client at any time during a period of 18 months after the alleged date of the notification as contemplated in paragraph 15.1.5 with the means to prove that such notification to the payment institution was made;

15.1.7 provide the client with an option to make a notification as contemplated in paragraph 15.1.5 free of charge, and ensure that any costs charged are directly attributed to the replacement of the payment instrument;

15.1.8 prevent any use of the payment instrument once notification has been made;

15.1.9 bear the operational and security risks of sending to the client a payment instrument or any personalised security credentials relating to it; and

15.1.10 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

Group B: Acquiring

16. Authorisation requirements for acquiring a payment activity

16.1 A person who seeks to conduct acquiring activity must apply to the Reserve Bank for authorisation as an acquirer.

16.2 An application under paragraph 16.1 must be submitted in the form as set out in Annexure C accompanied by the information prescribed therein.

16.3 The acquirer must meet the general requirements in paragraphs 2 to 4 and 6 to 8 of Annexure A.

16.4 In addition to the general requirements, a person who seeks authorisation as an acquirer must:

16.4.1 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in the Annexure D;

16.4.2 become a member of a PSMB or relevant authorised scheme(s), where such exists;

16.4.3 participate in relevant PCH arrangement(s);

16.4.4 be a clearing system participant or DCSP, or appoint a clearing system participant, DCSP or Reserve Bank settlement system participant to clear payment instructions on its behalf;

16.4.5 be a Reserve Bank settlement system participant or designated settlement system participant, or appoint a Reserve Bank settlement system participant or designated settlement system participant to settle payment obligations on its behalf;

16.4.6 open and maintain a formal beneficiary account, safeguard the client funds as set out in paragraph 9 of Annexure A, and provide evidence of such an account on application; and

16.4.7 register with the FIC as an accountable institution under item 23 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

16.4.8 commence with the acquiring of payment instructions activity within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank, failing which the authorisation would be automatically revoked.

17. Ongoing requirements for acquirers

17.1 An acquirer must:

17.1.1 enter into an agreement with a payee to govern the relationship between the acquirer and the payee, which, at the minimum, shall cover the following:

a. account maintenance, including updating and verifying information on business ownership and management;

b. business office and/or store address of payee, including the nature of the business;

c. timing (payment cycle) and manner of the transfer to the payee of the funds collected by the acquirer;

d. the classification by the payee of the means of receiving payment and payee account to which the funds will be transferred, as applicable;

e. disclosures and stipulations on the sharing of risks associated with acquiring between the acquirer and payee;

f. roles and responsibilities of each party, procedures and timelines;

g. liability management in case of negligence/security breaches/fraud, among others;

h. reconciliation process;

i. safeguards against unauthorised disclosure of client data and other protected information, data loss, fraud and cyber threats as well as arrangements to facilitate the secure and efficient sharing of data among authorised entities; and

j. handling and resolving complaints, refund/failed transactions or client returns;

17.1.2 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

17.1.3 comply with the requirements set out in paragraphs 5, 9, 10, 11, 12, 13 and 14 of Annexure A;

17.1.4 verify and record the identity of their payees and representatives, and comply with the AML/CFT/CPF requirements in Annexure K.

17.1.5 evaluate, analyse and periodically assess the overall potential risk of a payee;

17.1.6 ensure periodic monitoring of its payees in terms of adherence to their agreement and the payee's business activities;

17.1.7 keep records of these monitoring activities;

17.1.8 ensure transparency of charges/fees to payees;

17.1.9 maintain segregated bank accounts to hold funds received or collected on behalf of payees and ensure that such funds are safeguarded as per paragraph 9 of Annexure A and held separate from the acquirer's own funds The funds in segregated bank account/s must only be used for the payment of payees and/or transfers related to acquiring, including chargebacks or the charging of payee fees;

17.1.10 ensure the timely completion of payments with payees within the payment period agreed upon by the acquirer and the payee. The acquirer must safeguard the outstanding payee funds as set out in paragraph 9 of Annexure A; and

17.1.11 inform and notify the Reserve Bank, in writing, of any changes to the information submitted in the original application within thirty (30) business days of such change.

Group C: Payment execution – clearing, settlement and payment initiation

Category C1: Payment execution

18. Clearing

Application requirements for clearing

18.1 A person that is not a bank and who seeks to clear must apply to the Reserve Bank for designation to conduct clearing.

18.2 A person that is a bank and who seeks to clear must apply to the Reserve Bank for authorisation to conduct clearing.

18.3 An application under paragraph 18.1 and 18.2 must be submitted in a form as set out in Annexure C accompanied by the information prescribed therein.

18.4 A person that seeks designation or authorisation to clear must meet the general requirements in paragraphs 2 to 4 and 6 to 8 of Annexure A.

18.5 In addition to the general requirements, a person who seeks designation or authorisation to clear must meet and provide the following application requirements and information respectively:

18.5.1 at the time of application, hold minimum capital and comply with the prudential requirements as set out in Annexure D;

18.5.2 the business model of the applicant;

18.5.3 an indication of the types of payment instructions that the applicant will clear;

18.5.4 where a person seeking designation to clear is a non-bank, specify the Reserve Bank settlement system participant or participants associated with the person seeking designation to clear, who will settle payment obligations on behalf of the DCSP in the Reserve Bank settlement system, or obtain designation as a designated settlement system participant or appoint a designated settlement

system participant to settle its payment obligations in a designated settlement system;

18.5.5 where the person seeking authorisation to clear is a bank, confirm if it is a Reserve Bank settlement system participant or whether it will apply for and obtain authorisation as a Reserve Bank settlement system participant or designation as a designated settlement system participant to settle its payment obligations, or whether it will appoint another Reserve Bank settlement system participant or designated settlement system participant to settle payment obligations on its behalf in accordance with section 4(2)(d) and 4A of the NPS Act respectively;

18.5.6 where a Reserve Bank settlement system participant or designated settlement system participant has been appointed to settle payment obligations on behalf of a clearing system participant or DCSP, a signed letter from the Reserve Bank settlement system participant or designated settlement system participant confirming that it will settle the payment obligations on behalf of the clearing system participant or DCSP;

18.5.7 specify the PCHs, schemes and/or payment systems in which the person seeking designation or authorisation to clear seeks to participate;

18.5.8 obtain membership of the relevant PSMB or scheme(s), or be a participant in the relevant PCHs or payment system;

18.5.9 a bank clearing system participant and non-bank DCSP seeking to participate in a designated settlement system must obtain designation as a designated settlement system participant as set out in paragraph 20.1 below;

18.5.10 specify whether it will clear payment instructions on behalf of other payment institutions in terms of requirements outlined in paragraph 8; and

18.5.11 register with the FIC as an accountable institution under item 23 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

19. Ongoing requirements for clearing

19.1 A person that conducts clearing must, on an ongoing basis:

19.1.1 comply with requirements in paragraphs 5, 7 and 8 of Annexure A;

19.1.2 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

19.1.3 subsequent to the designation as a DCSP or authorisation to clear by the Reserve Bank, but prior to conducting clearing, obtain authorisation as a clearing system participant and be admitted as member of a PSMB in terms of section 4(5) of the NPS Act and in accordance with the entrance and participation criteria as well as authorisation requirements for clearing system participant and criteria for membership of the PSMB;

19.1.4 conclude service agreements with a PCH system operator through which clearing will be effected; and

19.1.5 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

20. Settlement

Application requirements for participation in the Reserve Bank settlement system and designated settlement system

20.1 A person who seeks to participate in the Reserve Bank settlement system or designated settlement system shall apply to the Reserve Bank for authorisation to participate in the Reserve Bank settlement system or designated settlement system.

20.2 An application under paragraph 20.1 shall be submitted in the form as set out in Annexure C and accompanied by the information prescribed therein.

20.3 A person that seeks authorisation to participate in a Reserve Bank settlement system or designated settlement system must meet the general requirements in paragraphs 2 to 4 and 6 to 8 of Annexure A.

20.4 In addition to the general requirements, a person who seeks authorisation to

participate in the Reserve Bank settlement system or designated settlement system shall meet the following requirements:

20.4.1 where a person seeks to participate in the Reserve Bank settlement system, such person must:

a. be the Reserve Bank, a bank, a mutual bank, a co-operative bank or a branch of a foreign institution or;

b. be admitted/authorised as a member of the PSMB; or

c. be a designated settlement system operator; and

d. meet the criteria for participation in the Reserve Bank settlement system as established by the Reserve Bank in consultation with the PSMB;

e. where a person seeks to participate in the designated settlement system, such person must be the Reserve Bank, a bank, mutual bank, a co-operative bank or a branch of a foreign institution or non-bank payment institution that is a DCSP;

20.4.2 specify the types of payment activities or payment obligations that will be settled in the Reserve Bank settlement system or designated settlement system;

20.4.3 obtain membership in the PSMB or relevant scheme(s) and/or participation in the relevant PCHs;

20.4.4 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in the Annexure D; and

20.4.5 meet the entry, participation and exit criteria, requirements and rules set out by the Reserve Bank settlement system operator or the designated settlement system operator.

21. Ongoing requirements for settlement system participants

21.1 A settlement system participant must, on an ongoing basis:

21.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

21.1.2 comply with the requirements in paragraphs 5, 10, 12, 13 and 14 of Annexure A;

21.1.3 where a settlement system participant appoints an agent or enters into outsourcing arrangements, comply with paragraphs 15 and 16 of Annexure A and provide information to the Reserve Bank as per Annexure F; and

21.1.4 inform and notify the Reserve Bank in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

22. Operation of a Reserve Bank settlement system

22.1 The Reserve Bank is exempted from applying for authorisation to operate the Reserve Bank settlement system.

22.2 Notwithstanding the exemption from authorisation, the Reserve Bank as the Reserve Bank settlement system operator must meet the general requirements in paragraphs 7, 8, 12 and 14 of Annexure A.

22.3 The Reserve Bank as the Reserve Bank settlement system operator must:

a. establish the entry, participation and exit criteria in consultation with the PSMB in accordance with section 3(4)(c) of the NPS Act, and subject to the approval of the Reserve Bank;
b. make and submit to the Reserve Bank, for approval, rules for participation in the Reserve Bank settlement system and dispute resolution rules;
c. admit Reserve Bank settlement system participants that comply with the criteria referred to in paragraph 22.3 (a);
d. enforce participation rules on Reserve Bank settlement system participants; and
e. with the prior approval of the Reserve Bank, terminate admission of a participant in the Reserve Bank settlement system.

22.4 The Reserve Bank may request the Reserve Bank settlement system operator to submit any amendments to the entry, participation and exit criteria and rules for review and approval.

22.5 The Reserve Bank may issue instructions to the Reserve Bank settlement system

operator, directing it to amend the rules in a particular manner to address issues identified by the Reserve Bank.

22.6 The Reserve Bank must ensure that the rules of the Reserve Bank settlement system operator include the following, at a minimum:

22.6.1 maintaining settlement accounts;

22.6.2 settlement finality;

22.6.3 risk mitigation;

22.6.4 liquidity provision;

22.6.5 operating procedures and times;

22.6.6 data protection and security; and

22.6.7 recovery of the Reserve Bank settlement system.

22.7 A Reserve Bank settlement system operator must:

22.7.1 develop and implement a robust risk management framework to identify, assess and manage its credit and liquidity risks arising from payment, clearing and/or settlement processes;

22.7.2 require its participants to maintain sufficient financial/prudential resources/capital/assets, including collateral where applicable, to fully cover credit or settlement exposure to each participant or other entities and liquidity pressures with a high degree of confidence;

22.7.3 establish rules and procedures to fully address any credit losses arising from individual or combined default among its participants concerning their obligations to the payment institution;

22.7.4 have rules that set out parameters for the circumstances in which specific resources of the participants can be used in the event of a participant default; and

22.7.5 pay interest on the funds held in a settlement account in the Reserve Bank settlement system or designated settlement system to the settlement account holder.

Category C2: Payment initiation

23. Payment initiation

23.1 This part applies to a payment initiation service provider and a payment account service provider that provides a payment account that is accessible electronically by the payer for the purposes of payment initiation.

23.2 **Authorisation requirements**

23.2.1 A person who seeks to provide a payment initiation activity shall apply to the Reserve Bank for authorisation as a payment initiation service provider.

23.2.2 An application under paragraph 23.2.1 shall be submitted in a form as set out in Annexure C accompanied by the information prescribed therein.

23.2.3 A person who seeks to provide a payment initiation activity must meet all the general requirements in Annexure A except paragraphs 9, 11, 12, 13 and 15.

23.3 In addition to the general requirements, a payment initiation service provider must:

23.3.1 at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in the Annexure D;

23.3.2 at all times, hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

23.3.3 comply with the technical standards as prescribed by the Reserve Bank;

23.3.4 not hold a payer’s funds in connection with the provision of payment initiation activity at any time, unless authorised to do so in terms of other payment activities that permit the holding of funds; and

23.3.5 on an ongoing basis, inform and notify the Reserve Bank, in writing, of any changes to the information submitted in the original application within thirty (30) business days of such change.

23.4 Data sharing

23.4.1 A payment initiation service provider must:

a. provide the service only after the payer has instructed the payment initiation service provider to initiate the payment instruction and has provided informed consent;

b. request client-consented data associated with the payment instruction, which must not include the payer's personalised security credentials issued by the payment account service provider to authenticate the payer;

c. transmit the payer's personalised security credentials in respect of payment initiated through safe and efficient channels, including encryption methods, and not make such personalised security credentials accessible to any other party except the payer and the issuer of the personalised security credentials;

d. identify itself towards the payment account service provider when initiating a payment instruction and communicate with the payment account service provider and the payer in a secure way as required by the authentication requirements referred to in paragraph 23.7;

e. not store the payer's sensitive payment data;

f. only request, from the payer, data for the purposes of payment initiation; and

g. not modify any information on the payment instruction unless the payer has provided informed consent.

23.4.2 A payment account service provider must:

a. communicate securely with the payment initiation service provider in accordance with the authentication requirements referred to in paragraph 23.7;

b. after receiving a payment instruction, timely provide or make available all the information regarding the payment instruction to the payment initiation service provider; and

c. not unfairly apply preferential treatment to the processing of a payment

instruction over any other payment instruction, except where prescribed by law.

23.4.3 A payment initiation service provider need not enter into a contractual relationship with a payment account service provider to provide payment initiation activity.

23.4.4 The same information, including confirmation of consent requested from the payer, must be provided by the payment initiation service providers to the payment account service providers.

23.5 Data security and privacy

23.5.1 A payment account service provider and payment initiation service provider must:

a. have adequate security measures to protect the confidentiality and integrity of payers' personalised security credentials;

b. ensure that the processing and routing of personalised security credentials and of the authentication codes takes place in secure environments in accordance with strong and commonly accepted industry standards;

c. comply with all requirements, where applicable, as provided for in the personal information and information protection laws, including but not limited to the POPI Act;

d. encrypt or mask the payer's personalised security credentials and ensure that they are not readable in plain text at the time when the payer is required to provide the credentials during the authentication;

e. use the commonly accepted and most robust industry encryption standards to secure the payer's personalised security credentials in transit;

f. use and regularly update anti-virus software to protect its systems from malware and data security breaches;

g. not store personalised security credentials in plain text within its database or

systems;

h. have adequate information and data security infrastructure and systems in place to prevent, detect and resolve any possible unauthorised access to the payer's information and/or data breach;

i. ensure that the creation of personalised security credentials is performed in a secure environment; and

j. mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying.

23.6 Provision and withdrawal of consent

23.6.1 A payment initiation service provider must:

a. have clear and simple consent management policies and processes for soliciting, managing and using client-consented data, which complies with the POPI Act. The process of collecting this data must be simple, standardised and secure, and includes the reason given for the purpose the data is collected;

b. keep a record of the provision and withdrawal of consent associated with payment instructions;

c. issue/initiate a payment instruction only when the payer has given informed consent for payment initiation. and

d. initiate/issue a series or scheduled payment instructions only when the payer has given informed consent.

23.6.2 Consent must not be used for any purpose except for the initiation of a payment instruction as explicitly requested by the payer.

23.6.3 A payer may withdraw consent at any time, provided that the withdrawal does not violate other legitimate obligations and/or the finality and irrevocability of the transaction required by the NPS Act.

23.6.4 Upon receiving a withdrawal of consent, the payment initiation service provider must immediately cease to initiate, schedule or submit any further payment instructions on behalf of the payer for which consent has been withdrawn.

23.6.5 In the absence of consent, a payment instruction shall be considered to be unauthorised.

23.7 Authentication

23.7.1 A payment account service provider must apply strong client authentication when the payer:

a. accesses the payment account online;

b. for every transaction, unless the payer has provided consent for a series of or scheduled payment instructions;

c. initiates apayment instruction; and

d. carries out any action through a remote channel, which may imply a risk of payment fraud or other abuses.

23.7.2 A payment account service provider must allow the payment initiation service provider to rely on the authentication procedures provided by the payment account service provider to the payer.

23.8 Centralised interface infrastructure

23.8.1 The Reserve Bank may appoint/approve the operator of a centralised interface infrastructure to manage the participation of payment initiation service providers and payment account service providers, including ensuring compliance with the technical standards prescribed by the Reserve Bank.

23.8.2 The operator of a centralised infrastructure must:

a. develop and implement a centralised interface infrastructure that enables payment account service providers, which provide payment accounts accessible online, to communicate with payment initiation service providers;

b. enable payment initiation service providers to identify themselves to the operator of a centralised infrastructure and to payment account service providers;

c. enable payment initiation service providers to securely initiate a payment instruction and receive information associated with the initiation of a payment instruction; and

d. ensure that the centralised interface infrastructure offers, at all times, the same level of availability, performance and support.

23.8.3 The centralised interface infrastructure must:

a. enable payment initiation service providers to rely on all the authentication procedures provided by the payment account service provider to the payer;

b. enable the payment initiation service provider to instruct the payment account service provider to authenticate the payer;

c. maintain the communication sessions between the payment account service provider, the payment initiation service provider and payer throughout the authentication process;

d. comply with technical standards applicable to payment initiation as prescribed by the Reserve Bank; and

e. maintain the integrity and confidentiality of the payer's personalised security credentials and of authentication codes transmitted by or through the payment

initiation service provider.

23.8.4 Contingency measures for centralised interface infrastructure

The operator of a centralised infrastructure must:

a. have a strategy and plans for contingency measures that can be used if the centralised interface infrastructure does not function due to unplanned unavailability or technical challenges;

b. have alternative interfaces that ensure that the payment initiation service providers and payment account service providers can be identified and authenticated;

c. inform payment initiation service providers and payment account service providers that use the centralised interface infrastructure about alternative interfaces that can be used when the centralised interface infrastructure is not functional; and

d. allow payment service providers to make use of an alternative interfaces until the centralised interface infrastructure is available and fully functional.

23.9 Alternative interface infrastructure

23.9.1 In the absence of a centralised interface infrastructure referred to in paragraph 23.8 above, a payment account service provider and a payment initiation service provider must develop and implement an interface infrastructure that enables:

a. the payment initiation service providers to identify themselves towards the payment account service providers; and

b. payment initiation service providers to securely initiate a payment instruction and receive all information on the issuing of the payment instruction.

c. a payment initiation service provider to rely on all the authentication procedures provided by the payment account service provider to the payer.

23.9.2 The alternate interface infrastructure must:

a. maintain the communication sessions between the payment account service provider, the payment initiation service provider and payer throughout the authentication;

b. comply with technical standards applicable to this payment activity as prescribed by the Reserve Bank; and

c. maintain the integrity and confidentiality of the payer's security credentials and of the authentication codes transmitted by or through the payment initiation service provider.

23.9.3 Contingency measures for the alternative interface infrastructure

a. The payment account service provider and payment initiation service provider must:

i. have a strategy and plans for contingency measures to be implemented where the interface infrastructure malfunctions due to unplanned unavailability or technical challenges;

ii. have alternative interfaces in place that ensure that other payment account service providers and payment initiation service providers can be identified and authenticated; and

iii. inform other payment account service providers and payment initiation service providers of alternative interfaces that may be used when the interface infrastructure is not functional.

23.9.4 Other payment account service providers and payment initiation service providers must be allowed to make use of the alternative interface until the interface infrastructure is available and fully functional.

23.9.5 In cases where the interface is unavailable and alternatives for sharing are

employed, the payment account service provider shall:

a. guarantee that the payment initiation service provider is not granted access to data or services other than those consented to by the payment services user; and

b. maintain a record of the accesses and data and services accessed by the alternative mechanism.

23.10 Liability risk management

23.10.1 A payment account service provider and payment initiation service provider must:

a. have effective mechanisms in place to detect and identify incidents of fraudulent or unauthorised access to payment accounts, payment instructions or incorrectly issued payment instructions, and conduct reviews of audit trails to identify the source of the incident to determine the party liable for losses; and

b. have in place necessary insurance or guarantee mechanisms against possible losses.

23.10.2 A payment account service provider must:

a. refund the payer, within 48 hours of confirming that a payment transaction was unauthorised or incorrectly facilitated, the amount of unauthorised or incorrectly facilitated payment instructions through the original method of payment, unless specifically agreed by the payer to have the refund processed through an alternate method of payment;

b. where a payer denies having authorised a payment instruction, provide supporting evidence that the informed consent or authentication was obtained from the payer, with the accurate payment amount, beneficiary name and transactional account number, and that the payment was not affected by technical deficiencies within its systems; and

c. where the payer acted fraudulently or with intent or gross negligence, provide supporting evidence to substantiate that the payer acted fraudulently, with

intent or gross negligence.

23.10.3 The payment initiation service provider must:

a. where a payer denies having authorised a payment instruction, provide supporting evidence that the informed consent or authorisation was obtained from the payer, with the accurate payment amount, beneficiary name and transactional account number, and that the payment was not affected by technical deficiencies within its systems;

b. where the payer acted fraudulently or with intent or gross negligence, provide supporting evidence to substantiate that the payer acted fraudulently, with intent or gross negligence; and

c. where it is liable for unauthorised or incorrectly initiated payment instruction, compensate the payment account service provider at its request, within 48 hours of confirming that a transaction or payment instruction was unauthorised or incorrectly facilitated, for the losses incurred as a result of the refund to the payer.

23.10.4 The payment account service provider must:

a. require the payer to utilise the payment instrument/account in accordance with the terms and conditions governing the issuance and usage of the payment instrument/account;

b. develop terms and conditions which are objective, non-discriminatory and proportionate;

c. provide mechanisms for the payment account service payer to notify it, without delay, on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument or personalised security credentials;

d. not hold the payer liable for any financial losses where the payment account service provider has not required strong client authentication, unless the payer has acted fraudulently;

e. ensure that the payer does not bear any losses resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with point (c), except where the payer has acted fraudulently; and

f. hold the payer liable for all the losses relating to any unauthorised payment transactions, provided the losses were incurred by the payer acting fraudulently or failing to fulfil the obligations set out in 23.12.3 and 23.12.4 with intent or gross negligence.

23.11 Dispute resolution mechanism

23.11.1 A payment account service provider and a payment initiation service provider must:

a. have a formal and fair dispute resolution mechanism in place, governed by processes, procedures and contractual arrangements that provide payers with practical means to lodge and resolve disputes relating to data access, management and usage, including, but not limited to, instances of fraud, unauthorised transactions, data breaches and misuse;

b. ensure that its dispute resolution mechanism, including the complaints handling facility, is clearly and easily accessible to payers through all applicable communication channels such as a phone line, email, mobile devices and a website;

c. ensure that the dispute resolution mechanism does not contravene the settlement provisions as stipulated in section 5 of the NPS Act; and

d. appoint an officer(s) responsible for the regulatory and payer complaints handling functions who shall promptly respond to all complaints raised and resolve the matter within a reasonable timeline.

23.11.2 Where disputes cannot be resolved between the payment institution and the payer, the matter may be escalated to the Reserve Bank or another relevant financial services ombudsman.

23.12 Payer education or awareness

23.12.1 A payment initiation service provider must:

a. prioritise payer education and digital financial literacy initiatives, particularly around data-sharing practices, consent management and dispute resolution;

b. raise awareness of the opportunities and risks within the data-sharing ecosystem, including data privacy, consent management and fraud prevention;

c. equip the payer with the knowledge, tools and confidence to actively manage their data and engage meaningfully with digital financial services, fostering trust, informed decisions and responsible usage; and

d. publicly disclose, in simple language, the terms and conditions for using its product or service, procedures for handling payer complaints, privacy policy and other terms and conditions, and these terms and conditions must be objective, non-discriminatory and proportionate.

23.13 Traceability, audit and record-keeping

23.13.1 A payment initiation service provider and a payment account service provider must:

a. have systems in place that ensure that each transaction is traceable;

b. have a robust internal and external audit function that will undertake an assessment of the effectiveness of its risk management and control processes;

c. be able to demonstrate, when requested by the Reserve Bank, that it applies robust data security standards, including data encryption; and

d. keep a record of every transaction, including the payer's informed consent, for at least five (5) years from the date on which that transaction is concluded. A transaction record must at a minimum include the amount involved, the date on which the transaction was concluded, the parties to the transaction, identifying particulars of all accounts and account files relating to each transaction, and the nature of the transaction.

Group D: Payments to third persons/third-party payment providers

24. Authorisation requirements for the provision of payments to third persons/TPPPs

24.1 A person who seeks to provide payments to third persons as set out in section 7(c) of the NPS Act on a large scale of R5 million and more in average monthly transaction values over a period of six (6) consecutive months, must apply to the Reserve Bank for authorisation as a Tier 1 TPPP.

24.2 A person who seeks to provide payments to third persons as set out in section 7(c) of the NPS Act on a limited scale of less than R5 million average monthly transaction values over a period of six (6) consecutive months must apply to the Reserve Bank for authorisation as a Tier 2 TPPP.

24.3 An application for 24.1 or 24.2 must be submitted in the form as set out in Annexure C and accompanied by the information prescribed therein.

24.4 At the time of authorisation, the person must hold minimum capital and comply with prudential requirements as set out in Annexure D.

25. A person who seeks authorisation to provide payments to third persons must meet the following requirements and provide the following information:

25.1 **Incorporation:** A duly registered and/or an incorporated juristic person in the RSA.

25.2 **Incorporation and registration:** Certified copies of the notice of incorporation and registration certificate issued by the Companies and Intellectual Property Commission (CIPC) under the Companies Act, 2008 (Act No. 71 of 2008) (Companies Act).

25.3 **Address:** The address of the applicant's place of business and head office in the RSA. Where applicable, if the applicant is also incorporated outside of the RSA, the address of the applicant's headquarters or parent company/entity in addition to the

address of their place of business and/or head office in the RSA.

25.4 **Business and operational plan:** A detailed business plan, including information on how the business model is funded, including own funds, loan funding and other sources of funding, and an operational plan outlining the specific type of third-party payment activity the applicant is applying for and the type of payment instructions that will be accepted.

25.5 **Financial position:** Applicants currently operating as TPPPs must submit audited financial statements for the past three (3) financial years and a financial forecast for the next three (3) years. Applicants who have not yet commenced operations as TPPPs are required to submit a financial forecast for the next three (3) financial years as outlined in Annexure D.

25.6 **Compliance Officer:** A curriculum vitae (CV) and identity document of the person appointed and responsible for the compliance function of a payment institution.

25.7 **Safeguarding of client funds:** Open and maintain a maximum of two formal beneficiary accounts and safeguard the client funds and provide evidence of such an account once authorised by the Reserve Bank.

25.8 **Registration with the FIC:** Applicants must register with the FIC as an accountable institution under item 19 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

26. Governance arrangements

26.1 Details of the applicant's governance arrangements must be provided, which have been approved by the governing body, senior management or highest level of authority, duly aligned with the prevailing best governance standards, principles, practices and internal control mechanisms.

27. Reporting requirements

27.1 By the end of February each year, a TPPP must submit the following data to the Reserve Bank for the period January to December of the preceding year:

27.1.1 the number of clients in the past 12 months;

27.1.2 aggregated annual volumes and values of payments to third parties processed;

27.1.3 aggregated annual amounts and maximum rand value deposited in segregated accounts in respect of payments to third parties;

27.1.4 duration of funds in the segregated accounts; and

27.1.5 an updated list of branches and agents, where applicable.

28. Fit-and-proper requirements

28.1 An applicant must, at application, submit a duly completed fit and proper declaration form, attached hereto as Annexure H, by each director and key person, and ensure that they remain fit and proper on an ongoing basis.

29. Risk management arrangements

29.1 An applicant must provide the following:

29.1.1 details of risk management measures, including a description of security controls and mitigation measures that have been or will be taken to protect payers, payees and the NPS from risks such as cyber incidents, suspected fraud, fraud and the illegal use of personal information; and

29.1.2 confirmation and a description of internal control mechanisms, including the Risk Management Compliance Programme, established to ensure compliance with the relevant AML/CFT/ counter-proliferation financing (CPF) measures as provided for in the legal frameworks of the POCA, the POCDATARA, the FIC Act and any relevant directives, regulations or notices issued under it.

30. Data protection

30.1 An applicant must:

30.1.1 provide details of how the confidentiality and integrity of payments data and systems will be protected, whether the data is in transit or stored;

30.1.2 ensure that appropriate protection and confidentiality arrangements are in place for data, information, systems and processes, in accordance with the POPI Act and applicable data protection laws;

30.1.3 implement measures to ensure that data and records maintained by a service provider or any third party remain the property of the applicant/payment institution; and

30.1.4 in the event that the data and records are maintained by a third party or service provider on behalf of the applicant or TPPP, provide their names and physical or registered business addresses.

31. Agency arrangements

31.1 A TPPP may use an agent/s to conduct a TPPP payment activity, subject to paragraph 15 of Annexure A.

32. Outsourcing arrangements

32.1 A TPPP that seeks to outsource its technology platform, internal audit and/or risk management functions as well as operational functions related to the provision of the TPPP payment activity under Annexure B must comply with paragraph 16 of Annexure A.

33. Ongoing requirements for authorised Tier 1 and Tier 2 TPPPs

33.1 A TPPP must, on an ongoing basis:

33.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

33.1.2 safeguard client funds as set out in paragraph 9 of Annexure A;

33.1.3 comply with the requirements in paragraphs 5, 6, 11, and 13 of Annexure A;

33.1.4 comply with the AML/CFT/CPF requirements in Annexure K;

33.1.5 commence engagement in providing payments to third persons within 12 months

from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank. Failure to commence money remittance within the 12-month period shall render the authorisation automatically revoked.

33.1.6 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change; and

33.1.7 prior to entering into a business relationship or agreement, at a minimum:

a. obtain and verify the certified hard or electronic copies of the business registration and/or founding documents of its clients issued by the relevant authorities;

b. obtain and verify the certified hard or electronic copies of the identity documents of the directors, shareholders and beneficial owners of its clients;

c. obtain a certified hard or electronic copy of the proof of physical or business address that is not older than three months;

d. confirm that the contact details of its clients are correct;

e. conduct reference checks of its clients; and

f. ensure they have adequate systems in place that can technically integrate with the system of the payer or beneficiary, as the case may be.

33.2 Where the segregated bank account holding client funds earns interest as set out in paragraph 11 of Annexure A, such interest shall accrue to the TPPP and shall not be paid to the client.

33.3 The TPPP must make payment to a beneficiary or payee in accordance with the frequency and timeline as agreed between the TPPP and its client, provided that beneficiary or payee funds are not held for more than 30 days after receipt of payment(s) from the payer(s).

34. Ongoing funds management requirements for authorised Tier 1 and Tier 2 TPPPs

34.1 When receiving funds from multiple payers to pay out the aggregated value as a single transaction to a beneficiary, the TPPP must record each underlying transaction. Each record of the underlying transaction must include a transaction reference number, transaction date, payer's name and surname (or registered name if the payer is a juristic person), the amount in rand and the name of the relevant beneficiary. These records must be retained for five (5) years from the date the transaction was processed.

34.2 When receiving funds from a payer as a single transaction to distribute to multiple beneficiaries, the TPPP must record each underlying transaction with a transaction. Each record of the underlying transaction must include a transaction reference number, transaction date, beneficiary's name and surname (or registered name where the beneficiary is a juristic person), the amount in rand and the name of the relevant payer. These records must be retained for five (5) years from the date the transaction was processed.

34.3 The TPPP must keep separate and distinct the business divisions of that person who provides payments to third persons from the other business divisions of that person who provides system operator services.

34.4 Once the person making payments to third persons/parties or its duly appointed agent receives payments from multiple payers on behalf of the beneficiary client to whom the payment is due, the payment obligation of the multiple payers to the beneficiary is deemed to have been discharged or satisfied.

34.5 Where a person making payments to third persons/parties or its duly appointed agent receives payments from a payer to pay to multiple beneficiaries to whom the payment is due, the payment obligation of the payer shall be deemed to be discharged or satisfied once the beneficiaries have received the payment.

Group E: Schemes

35. Authorisation requirements for managing a scheme

General application requirements to manage a scheme

35.1 A person seeking to manage a scheme must apply to the Reserve Bank for authorisation as a scheme manager.

35.2 An application under paragraph 35.1 shall be submitted in the form as set out in Annexure C accompanied by the information prescribed therein

35.3 A person who seeks authorisation to manage a scheme must meet the general requirements in paragraphs 2 to 4, 6 and 8 of Annexure A.

35.4 In addition to the general requirements, a person who seeks authorisation to manage a scheme must meet the following requirements:

35.4.1 indicate the payment instruments/systems the scheme will be supporting;

35.4.2 provide volumes and values that were processed for the last three (3) years or the projected annual volumes and values for the next three (3) years;

35.4.3 keep the business of the scheme separate from clearing business/activities;

35.4.4 comply with applicable standards and practices for information technology (IT) security standards, data and information security management systems for cyber protection and data protection, where applicable;

35.4.5 develop rules on branding, risk management, clearing and settlement (payment of users/sub-users) relating to the scheme;

35.4.6 develop and implement a comprehensive framework for risk (including operational risk and risk that can affect the payment network) and fraud management, which should include the identification, management and mitigation measures for managing a scheme; and

35.4.7 disclose its fees to its members and avoid bundling of scheme and clearing/processing fees.

36. Establishment of criteria and rules

36.1 A person seeking to manage a scheme must:

36.1.1 establish the entry, participation and exit criteria for its members and submit such criteria to the Reserve Bank for approval;

36.1.2 make and submit to the Reserve Bank for review and/or approval the rules for members of its scheme, including dispute resolution rules;

36.1.3 admit scheme members that comply with criteria referred to in 36.1.1;

36.1.4 enforce those rules in relation to its scheme members; and

36.1.5 with the prior approval of the Reserve Bank, terminate membership of a member in a scheme, in accordance with the scheme rules.

36.2 The Reserve Bank may request the submission of any amendments to the entry, participation and exit criteria and rules for review and/or approval.

36.3 Where the Reserve Bank issues an instruction to the manager of a scheme, directing it to amend the rules in a particular manner to address issues identified by the Reserve Bank, the scheme manager must comply with such instructions issued by the Reserve Bank to amend the rules accordingly.

37. Ongoing requirements for schemes

37.1 The scheme must comply with the requirements set out in paragraph 10 of Annexure A:

37.1.1 submit annual volumes and values that were processed per payment activity.

37.2 Information security

37.2.1 A scheme manager shall apply and meet at a minimum the data security standards to ensure compliance with paragraph 8 of Annexure A and applicable legislation.

37.2.2 The cybersecurity and cyber-resilience policy, strategy and framework outlining the cybersecurity and cyber-resilience measures, processes procedures and controls that the scheme must comply with the applicable legislation and directives

in respect of cybersecurity and cyber-resilience.

37.3 **Disaster recovery and business continuity management**

37.3.1 A scheme manager must have disaster recovery and business continuity plans in place to ensure their ability to manage a scheme on an ongoing basis and limit losses in the event of severe business disruption. Such plans must be commensurate with the risk profile, nature, size and complexity of the scheme's business and structure, and must take into account different scenarios to which the scheme may be vulnerable.

37.3.2 Disaster recovery and business continuity plans shall ensure that critical business functions of the scheme can be maintained and recovered in a timely manner to minimise the financial, legal, regulatory, reputational and other risks that may arise from a disruption.

37.3.3 The governing body must ensure there is a periodic independent review of the scheme's disaster recovery and business continuity plans to ensure adequacy and consistency with current operations, risks and threats, recovery levels and priorities.

37.4 **Risk assessment**

37.4.1 A scheme manager must regularly assess risks through the identification of new risks, measurement of known risks and prioritisation of risks through thorough understanding of the business and the market.

37.5 **Risk mitigation**

37.5.1 A scheme manager must mitigate risks through the

a. risk mitigation programmes and technologies;

b. effective management of risk principles;

c. operation with risk management in mind; and

d. outsourcing of risk functions that cannot be performed in-house.

37.6 **Monitoring**

37.6.1 A scheme manager must perform regular monitoring of all risks and mitigation programmes on at least an annual basis to ensure the robustness of the risk

management procedures and programmes. Continuous monitoring reports, including dashboards, shall be presented to the senior management and the governing body of the scheme to ensure that all levels of senior management are aware of the current risk situation, including potential fraud, in relation to the management of the scheme.

37.7 A scheme manager must inform and notify the Reserve Bank, in writing, of any changes to the information submitted in the original application within thirty (30) business days of such change.

Group F: Money remittance

38. Authorisation requirements for Tier-1 money remitter/money remittance payment activity

Tier 1 money remittance

38.1 A person who seeks to conduct money remittance on a large scale of R5 million and more in average monthly liabilities over a period of six (6) consecutive months, must conduct the money remittance in an interoperable payment system and apply to the Reserve Bank for authorisation as a Tier 1 money remitter.

38.2 An application under paragraph 38.1 shall be submitted in the form as set out in Annexure C accompanied by the information prescribed therein.

38.3 A Tier 1 money remitter must meet the requirements in paragraphs 2 to 4, 6 to 8 and 17 of Annexure A of this Directive.

38.4 In addition to the general requirements, a person who seeks authorisation as a Tier 1 money remitter:

38.4.1 must, at the time of authorisation, hold minimum capital and comply with the prudential requirements as set out in Annexure D; and

38.4.2 may conduct money remittance from cash or funds in the payment account, e-

money and/or card sent by or received from its client or any other payment instrument as approved by the Reserve Bank.

38.5 A Tier 1 money remitter that provides single money remittance transactions or that establishes a business relationship with a client/payer to provide money remittance shall ensure that daily transaction values do not exceed R5 000 per client/payer with a limit of R50 000 per client/payer per calendar month.

38.6 A Tier 1 money remitter must transfer to the payee all funds in real time but no later than close of business day.

38.7 Where, due to unforeseen or exceptional circumstances, the client funds are still held by the payer money remitter and not yet transferred to the payee or payee money remitter by the end of the business day of receipt of the funds, such funds must be kept in a segregated bank account and safeguarded as set out in paragraph 9 of Annexure A.

38.8 A Tier 1 money remittance must:

38.8.1 where a Tier 1 money remitter is a non-bank, be designated as a clearing system participant by the Reserve Bank, or, where a Tier 1 money remitter is a bank, be authorised as a clearing system participant by the Reserve Bank and the PSMB or appoint a clearing system participant or DCSP to clear on its behalf subject to compliance with the sponsorship requirements as set out in paragraph 8;

38.8.2 where a Tier 1 money remitter is either a bank or a non-bank, be authorised as a member of a PSMB or scheme and participate in the relevant PCH or scheme or appoint an authorised PSMB or scheme member to participate in the relevant PCH or scheme on its behalf;

38.8.3 meet the entry and participation requirements for settlement system participants as set out in this Directive and by the Reserve Bank settlement system operator as approved by the Reserve Bank to settle payment obligations linked to its payment activity or appoint a Reserve Bank settlement system participant to settle payment obligations on its behalf as required by section 4(2)(d) of the NPS Act if settlement is in the Reserve Bank settlement system, or be designated as a

settlement system participant or appoint a designated settlement system participant to settle payment obligations on its behalf;

38.8.4 comply within and in accordance with the clearing and settlement requirements and timelines duly aligned to the clearing and settlement requirements as provided for in the NPS Act and directives, PCH agreements, settlement agreements, clearing and settlement rules, clearing and settlement operational procedures or relevant instrument(s) issued by the PSMB, the PCH system operators and operators of settlement systems, as the case may be;

38.8.5 register with the FIC as an accountable institution under item 19 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

39. Ongoing requirements for Tier 1 money remitters

39.1 A Tier 1 money remitter must comply with the following requirements on an ongoing basis:

39.1.1 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

39.1.2 comply with the requirements in paragraphs 5 to 14 of Annexure A;

39.1.3 comply with the AML/CFT/CPF requirements in Annexure K;

39.1.4 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change;

39.1.5 must notify the Reserve Bank, in writing, immediately after opening a money remittance branch;

39.1.6 where the Tier 1 money remitter appoints an agent or enters into outsourcing arrangements, comply with paragraphs 15 and 16 of Annexure A and F; and

39.1.7 commence engagement in money remittance within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank.

39.2 Failure to commence money remittance within the 12-month period shall render

the authorisation automatically revoked.

39.3 Where a client has more than one account with a money remitter, the money remitter must ensure that the total balance of all these accounts does not exceed the limits specified in paragraph 38.5.

39.4 A money remitter shall not permit or process transactions that appear to be deliberately split into small amounts to circumvent the transaction limits specified in paragraph 38.5.

39.5 A money remitter must transfer to the payee all funds in real time but no later than close of business.

39.6 A money remitter must provide evidence of such an account.

39.7 Where, due to unforeseen or exceptional circumstances, the client funds were received from the payee money remitter or its agent, and are still held and not yet transferred to the payee by the end of the business day following the day of receipt of the funds, the payee money remitter must keep such funds in a formal beneficiary account and safeguarded as set out in paragraph 9 of Annexure A.

39.8 A money remitter must at all times demonstrate that it can reconcile the funds paid into its clients' segregated bank account with a specific client transaction executed.

Tier 2 money remittance

40. Application requirements for Tier 2 money remitters

40.1 A person who seeks to conduct interoperable money remittances on a limited scale of less than R5 million in average monthly liabilities over a period of six (6) months, must apply to the Reserve Bank for authorisation as a Tier 2 money remitter.

40.2 An application under paragraph 40.1 shall be submitted in the form as set out in the Annexure C accompanied by the information prescribed therein.

40.3 A person who seeks authorisation as a Tier 2 money remitter must meet the application requirements in paragraphs 2 to 4, 6 to 8 and 17 of Annexure A.

40.4 In addition to the general requirements, a person who seeks authorisation as a Tier 2 money remitter must meet the following requirements:

40.4.1 at the time of authorisation, such a person must hold the minimum capital and comply with the prudential requirements as set out in Annexure D;

40.4.2 may conduct money remittance using cash or funds from a payment account, e-money and/or cards sent by or received from its client or any other payment instrument as approved by the Reserve Bank; and

40.4.3 the person provides evidence of the bank account that will be utilised and segregated to safeguard client funds as set out in paragraph 9 of Annexure A.

40.5 Where a Tier 2 money remitter is a non-bank, it must be designated as a clearing system participant by the Reserve Bank, or, where a Tier 2 money remitter is a bank, it must be authorised as a clearing system participant by the Reserve Bank and the PSMB or appoint a clearing system participant or DCSP to clear on its behalf subject to compliance with the sponsorship requirements as set out in paragraph 8.

40.6 Where the Tier 2 money remitter is either a bank or a non-bank, it must:

40.6.1 be authorised as a member of a PSMB and participate in the relevant PCHs/scheme or appoint an authorised PSMB member to participate in the relevant PCH/scheme on its behalf;

40.6.2 meet the entry and participation requirements for settlement system participants as set out in this Directive and by the Reserve Bank settlement system operator as approved by the Reserve Bank to settle payment obligations linked to its payment activity or appoint a Reserve Bank settlement system participant to settle payment obligations on its behalf in accordance with section 4(2) (d) of the NPS Act, subject to compliance with the sponsorship requirements under paragraph 8, if settlement is in the Reserve Bank settlement system, or be designated as a settlement system participant or appoint a designated settlement system participant to settle payment obligations on its behalf subject to compliance with the sponsorship or indirect access requirements under paragraph 8;

40.6.3 comply with the clearing and settlement requirements and timelines duly aligned to the clearing and settlement requirements as provided for in the NPS Act and directives, PCH agreements, settlement agreements, clearing and settlement rules, clearing and settlement operational procedures or relevant instrument(s) issued by the PSMB, the PCH system operators and operators of settlement systems, as the case may be; and

40.6.4 register with the FIC as an accountable institution under item 19 of Schedule 1 of the FIC Act, within thirty (30) business days of issuance of the authorisation.

41. Ongoing requirements for Tier 2 money remitters

41.1 A Tier 2 money remitter must comply with the following requirements on an ongoing basis:

41.1.1 A Tier 2 money remitter that conducts single money remittance transactions or that establishes a business relationship with a client to provide money remittance shall ensure that each transaction does not exceed R2 500 per day per client with a limit of R25 000 per client per calendar month, or as may be amended by the Reserve Bank from time to time;

41.1.2 hold ongoing capital and comply with the prudential requirements as set out in Annexure D;

41.1.3 notify the Reserve Bank, in writing, immediately after opening an outlet or branch;

41.1.4 where a client has more than one account with a money remitter, ensure that the total balance of all these accounts does not exceed the limits specified in paragraph 41.1.1;

41.1.5 not permit or process transactions that appear to be deliberately split into small amounts to circumvent the transaction limits specified in paragraph 41.1.1;

41.1.6 transfer to the beneficiary all funds in real time but no later than close of business day;

41.1.7 where, due to unforeseen or exceptional circumstances the client funds were received from the payee money remitter or its agent, and are still held and not yet

transferred to the payee by the end of the business day of receipt of the funds, the payee money remitter must keep such funds in a formal beneficiary account and safeguarded as set out in paragraph 9 of Annexure A. The Tier 2 money remitter must provide evidence of such an account;

41.1.8 always be able to demonstrate that it can reconcile the funds paid into its clients' segregated account with a specific client transaction executed;

41.1.9 comply with the requirements under paragraphs 7 to 14 of Annexure A;

41.1.10 comply with paragraph 15 of Annexure A as well as Annexure F if it intends to enter into agency business;

41.1.11 comply with paragraph 16 of Annexure A if it intends to enter into outsourcing arrangements;

41.1.12 comply with the AML/CFT/CPF requirements in Annexure K;

41.1.13 commence actual engagement in money remittance within 12 months from the date of issuance of the authorisation, unless a longer period has been approved by the Reserve Bank (Failure to commence actual money remittance within the 12-month period shall render the authorisation automatically revoked); and

41.1.14 inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

Part 4: Closed-loop payment system or payment activities

42. Registration requirements for closed-loop payment system or payment activity

42.1 A person may operate a closed-loop payment system or conduct closed-loop payment activities:

42.1.1 through a sponsorship arrangement with an authorised or a designated payment institution, in accordance with paragraph 8 of this Directive, provided that the sponsoring payment institution obtains prior written approval of the Reserve Bank of the sponsorship arrangements and subject to the provisions of paragraph 42.2; or

42.1.2 directly without a sponsorship arrangement subject to the provisions of paragraph 42.3.

42.2 An authorised payment institution that sponsors the operation of a closed-loop payment system or conduct of a closed-loop payment activity as set out in paragraph 42.1.1 must apply for registration to the Reserve Bank in the relevant form as set out in Annexure C in respect of the sponsored closed-loop payment system or payment activity, and must comply with and ensure compliance by the sponsored operator of closed-loop payment system or payment activity provider with paragraphs 42 and 43 of this Directive.

42.3 A person seeking to conduct a closed-loop payment system or payment activity set out in 42.1.2 must apply for registration to the Reserve Bank in the relevant form as set out in Annexure C and comply with paragraphs 42 and 43.

42.4 The following is included in the scope of a closed-loop payment system and payment activity which requires registration:

42.4.1 the issuance of payment instruments or e-money (the issuance of stores of value);

42.4.2 money remittance; and

42.4.3 payment instruments which can be redeemed for cash, including:

a. the use of private label cards (prepaid or post-paid) accepted only at the

issuer's store, affiliated chain stores or ecosystem;

b. prepaid/post-paid instruments accepted within a network of merchants under the same brand identity (e.g. franchises);

c. instruments issued and accepted exclusively in a three-party payment scheme intended solely for payment;

d. fuel cards, membership cards, public transport cards, meal vouchers and others;

e. shopping vouchers and electronic gift cards (where e-vouchers for a specific mall or a single merchant are considered limited purpose); and

f. loyalty and reward programmes (where points or stored value from airline frequent flyer programmes, retail loyalty cards or club memberships fall into the category of closed-loop payment activities).

42.5 The application for registration must be accompanied by supporting documentation or information, which includes, but is not limited to, the following:

42.5.1 in the case of paragraph 42.1.2, the name of the person seeking to operate a closed-loop payment system or conduct a payment activity, or, in the case of paragraph 42.1.1, the name of the sponsoring payment institution and the person to be sponsored to operate a closed-loop payment system or conduct a payment activity, hereinafter referred to as 'the applicant';

42.5.2 certified copies of the notice of incorporation and registration certificate issued by the CIPC under the Companies Act;

42.5.3 the address of the applicant's place of business and head office in the RSA;

42.5.4 the main business of the applicant;

42.5.5 a direct contractual agreement for acceptance of payment transactions concluded between the issuer of the payment instrument and each provider of goods and services, and, where applicable, each acceptor operating within the limited network;

42.5.6 details of the closed-loop payment system or payment activities, including end-to-end payment flow;

42.5.7 risk and fraud identification, management and mitigation measures of operating or the provision of closed-loop payments activities;

42.5.8 the opening and maintaining of a segregated bank account to safeguard client funds on an ongoing basis and providing evidence of such an account;

42.5.9 specifying the locations and/or specific geographical area where a closed-loop payment system will be operational;

42.5.10 envisaged number of providers of goods and services operating within a closed-loop payment system;

42.5.11 a common brand that characterises a closed-loop payment system;

42.5.12 the volume and value of payment transactions to be executed on an annual basis, as envisaged by the issuer;

42.5.13 the maximum amount to be credited to the payment instruments, as envisaged by the issuer;

42.5.14 the maximum number of payment instruments or e-money to be issued, as envisaged by the issuer;

42.5.15 details of the targeted segments and benefits of a closed-loop payment system and payment activities;

42.5.16 audited financial statements for the past three (3) years and a financial forecast for the next three (3) years. Applicants who have not yet commenced as operators of closed-loop payment systems are required to submit a financial forecast for the next three (3) financial years;

42.5.17 confirmation and a description of internal control mechanisms, including the Risk Management Compliance Programme, established to ensure compliance with the relevant AML/CFT/CPF measures as provided for in the legal frameworks of the

POCA, the POCDATARA, the FIC Act and any relevant directives, regulations or notices issued under it;

42.5.18 details of the agents used (if applicable); and

42.5.19 details relating to paragraph 17 of Annexure A.

42.6 The total value of payment transactions executed per payment activity in a closed-loop payment system over the preceding 12 months or forecast over 12 months must not exceed the amount of R15 million and/or 1 million customers.

42.7 Where the transactions exceed R15 million and/or 1 million customers, the operator or provider of the closed-loop payment system payment activities must notify the Reserve Bank, in writing, to assess whether or not the operator of a closed-loop payment system must apply for authorisation as a payment institution to operate or provide the payment activity in the interoperable environment.

42.8 Persons that conduct payment activities within the closed-loop payment system must register with the FIC as an accountable institution under item 19 of Schedule 1 of the FIC Act, within thirty (30) business days of registration.

42.9 Persons that operate a closed-loop payment system or conduct payment activities within the closed-loop payment system must apply for authorisation within thirty (30) days of exceeding the prescribed threshold or as directed by the Reserve Bank.

43. Ongoing requirements for the provision of closed-loop payment system and payment activity

43.1 The applicant must comply with the requirements as set out in paragraphs 9, 10, 12 and 13 of Annexure A.

43.2 The payee's payment account service provider must ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount has been credited to that payment account service provider's account.

43.3 comply with the AML/CFT/CPF requirements in Annexure K

43.4 Inform and notify the Reserve Bank, in writing, of any amendments to the information provided in their initial application within thirty (30) business days of the change.

Part 5: Reserve Bank powers and responsibilities

44. Regulation, oversight and supervision

44.1 The Reserve Bank shall exercise regulation, oversight and supervision as well as enforcement over a payment institution.

44.2 The Reserve Bank – in its capacity as regulator, overseer and supervisor of the NPS – must have access to any information as described in section 10 of the NPS Act and relating to a payment system and the Reserve Bank settlement system, and any person must on request provide such information to the Reserve Bank in such form and at such times as the Reserve Bank may require.

44.3 A payment institution, sponsored payment institution, sponsored institution, agent and master agent must give access to the Reserve Bank to review their systems and databases in terms of section 10 of the NPS Act.

44.4 The Reserve Bank may:

44.4.1 request any information from a sponsored payment institution, sponsored institution, an agent, master agent or payment institution;

44.4.2 conduct inspections of the books and premises of a sponsored payment institution, sponsored institution, an agent, master agent or payment institution;

44.4.3 direct a sponsored payment institution, sponsored institution, an agent, master agent or payment institution to take a specific action or cease conduct;

44.4.4 direct a payment institution to terminate the agency agreement or sponsorship arrangements; and

44.4.5 direct a payment institution to take remedial action based on the conduct of an agent or master agent.

44.5 The Reserve Bank shall regulate, supervise and oversee persons tasked with performing functions through sponsorship arrangements and agency

arrangements. This includes conducting supervisory on-site inspections and investigations as well as issuing directives to ensure that these functions comply with the NPS Act, this Directive and any other prescribed requirements which the Reserve Bank may issue.

44.6 The Reserve Bank may publish an updated list of agents on its website, which will be updated regularly.

45. Supervision and compliance monitoring of payment institutions

45.1 The Reserve Bank may at any time conduct a supervisory on-site or off-site inspection or audit on payment institutions, in the form and manner that the Reserve Bank may determine, to promote compliance with this Directive.

45.2 Subject to subparagraph 45.4, the Reserve Bank must provide at least fourteen (14) days' written notification to the payment institution whose business premises will be inspected prior to conducting the supervisory on-site inspection.

45.3 The supervisory on-site inspection notification must specify:

45.3.1 the date(s) of the intended supervisory on-site inspection;

45.3.2 the names of the Reserve Bank representatives;

45.3.3 the period for which the institution will be under review; and

45.3.4 any other information/documentation required for inspection purposes.

45.4 In addition, each Reserve Bank representative may produce a letter of authority on the Reserve Bank letterhead and identity document upon entry at the premises of a payment institution for verification purposes. Such representatives are not permitted to produce copies of these documents.

45.5 The Reserve Bank representatives may enter the premises of payment institutions:

45.5.1 without prior consent for business premises operated by payment institutions;

45.5.2 with prior consent for a private residence if the business of the payment institution is reasonably believed to be conducted there; or

45.5.3 without prior consent and notice to any payment institution if the entry is authorised by:

a. a warrant in terms of paragraph 45.11; or

b. a senior staff member of the Reserve Bank if the senior staff member on reasonable grounds believes that:

i. a warrant will be issued if applied for, in terms of paragraph 45.11;

ii. the delay in obtaining the warrant is likely to defeat the purpose for which entry of the premises is sought; and

iii. it is necessary to enter the premises to conduct the inspection and search the premises.

45.6 While on the premises, the Reserve Bank representatives, for the purpose of conducting the inspection, have the right to access any part of the premises and to inspect any document or item on the premises, and may do any of the following:

45.6.1 open or cause to be opened any strongroom, safe, cabinet or other container in which the Reserve Bank representatives reasonably suspect there is a document or item that may be relevant to the inspection;

45.6.2 examine, make extracts from and copy any document on the premises;

45.6.3 question any person on the premises to find out information relevant to the inspection;

45.6.4 require a person on the premises to produce to the Reserve Bank representatives any document or item that is relevant to the inspection and is in the possession or under the control of the person;

45.6.5 require a person on the premises to operate any computer or similar system on or available through the premises to:

a. search any information in or available through that system; and

b. produce a record of that information in any format that Reserve Bank representatives reasonably require;

45.6.6 if not practicable or appropriate to meet a requirement in terms of subparagraph 45.6.5, operate any computer or similar system on or available through the premises for a purpose set out in that subparagraph; and

45.6.7 take possession of, and take from the premises, a copy of any document or item that may afford evidence of a contravention of this Directive or may be relevant to the inspection.

45.7 The Reserve Bank representatives must give the person apparently in charge of the premises a written and signed receipt for the copies of documents or items taken as mentioned in paragraph 45.6.

45.8 A payment institution from whose premises a document or item was taken as mentioned in paragraph 45.6, or its authorised representative, may, during normal office hours and under the supervision of the representatives of the Reserve Bank, examine, copy and make extracts from a document or item.

45.9 A person who is questioned or required to produce a document or information during a supervisory on-site inspection may object to do so if they believe that their response, the document or the information may potentially incriminate them.

45.10 On such an objection, the Reserve Bank representative conducting the supervisory on-site inspection may insist on compliance, in which case the person must answer the question or produce the requested document or information.

45.11 A judge or magistrate may issue a warrant under this paragraph if:

45.11.1 the Reserve Bank submits a written application, setting out, under oath or affirmation, why it is necessary to enter and inspect the premises; and

45.11.2 the magistrate or judge believes, from the information provided under oath or affirmation, that:

a. there are reasonable grounds to suspect that a contravention of the Directive has occurred, is occurring or may occur;

b. entering and searching the premises is likely to yield information pertaining to

the contravention; and

c. entering and searching those premises is reasonably necessary for the investigation.

45.12 A warrant issued under paragraph 45.11 must be signed by the issuing judge or magistrate.

45.13 Reserve Bank representatives that enter the premises under the authority of a warrant must:

45.13.1 if no one is apparently in charge of the premises when the warrant is executed, fix a copy of the warrant on a prominent and accessible place on the premises; and

45.13.2 on reasonable demand from anyone present, produce the warrant or a copy of the warrant.

45.14 Payment institutions must retain full responsibility and accountability to comply with this Directive and may not delegate accountability to another institution, agent or service provider. This includes compliance with the NPS Act, all regulatory instruments issued in terms of the NPS Act and other financial sector laws.

45.15 Payment institutions must not prevent or inhibit the Reserve Bank from effectively performing its duties to effectively regulate, supervise and oversee their activities, systems, data and operations related to authorised, designated and registered payment activities.

46. Supervisory interventions

46.1 When the Reserve Bank is of the opinion that a payment institution:

46.1.1 risk profile does not adequately reflect:

a. the nature, scale, complexity or risk profile of its activities;
b. external factors that may materially affect the entity, including market conditions or operational dependencies;

c. risks associated with specific activities or services, including operational, settlement, liquidity, cyber, consumer protection or financial crime risks;
d. risks arising from a type or group of transactions, customers or service arrangements;

46.1.2 financial resources, safeguards or risk mitigation measures are likely to be overstated or insufficient, including where such resources are subject to material volatility or uncertainty;

46.1.3 policies, governance arrangements, processes or procedures relating to risk identification, assessment and management are inadequate;

46.1.4 internal controls, compliance arrangements or operational resilience measures are inadequate, the Reserve Bank may, among other things, require the payment institution:

a. to maintain additional capital requirements or safeguards, calculated and subject to such conditions as may be specified in writing by the Reserve Bank;
b. to restrict, suspend or modify specific activities, services or transaction types;
c. to strengthen or remediate its governance, risk management, compliance or control arrangements; and
d. to implement any other supervisory measure deemed necessary to ensure compliance with the Authorisation Framework and the integrity, safety and efficiency of the national payment system.

47. Variation, suspension and revocation of authorisation, designation, registration, sponsorship arrangements and exemptions

47.1 The Reserve Bank may vary the authorisation, designation, sponsorship arrangements or exemption of a payment institution, collectively referred to herein as ‘the participation mechanism’, including:

47.1.1 varying the condition of a participation mechanism;

47.1.2 adding a condition;

47.1.3 changing the name of the payment institution, where applicable; and

47.1.4 changing the payment activities to which the participation mechanism relates.

47.2 The Reserve Bank may issue a notice to a payment institution to suspend its participation mechanism for a specified period if it is satisfied, based on all available information, that:

47.2.1 the payment institution no longer meets the requirements outlined in this Directive or the participation mechanism conditions; and

47.2.2 the suspension is necessary to prevent a contravention of the NPS Act.

47.3 The Reserve Bank may revoke the participation mechanism of a payment institution if the payment institution:

47.3.1 submitted misleading and/or false information in its application;

47.3.2 no longer complies with the NPS Act and the participation mechanism requirements or conditions;

47.3.3 engages in payment activities that threaten the stability, efficiency and/or integrity of the NPS; and

47.3.4 fails to use its authorisation, designation or registration within 12 months after it was granted.

47.4 Prior to the Reserve Bank varying, suspending or revoking a participation mechanism, it must:

47.4.1 notify the payment institution of the proposed action and the reasons for it; and

47.4.2 invite the payment institution to make submissions on the matter and give it a reasonable period to do so.

47.5 The period referred to in paragraph 47.4.2 must be at least one (1) month.

47.6 The Reserve Bank need not comply with paragraph 47.4.1 and 47.4.2 if the payment institution has applied for the variation, revocation or suspension.

47.7 The Reserve Bank shall publish, on its website, the notices relating to the variation,

suspension or revocation of authorisation and exemption.

48. Conclusion

48.1 This Directive is not exhaustive and may be supplemented and/or amended from time to time.

48.2 All participants that provide domestic payment activities listed in Annexure B as well as closed-loop payment activities in terms of paragraph 42 are obliged to act in accordance with this Directive. Any contravention of this Directive is an offence in terms of section 12 of the NPS Act.

48.3 This Directive will become effective within three (3) months from the date of publication. Entities that are already governed or designated under the NPS Act, or in terms of Directives issued in terms thereof, are required to apply for authorisation in terms of the transitional arrangements specified in Annexure E.

48.4 Participants that are uncertain as to whether their current and/or future business practices are aligned with this Directive must initiate discussions with the Reserve Bank's National Payment System Department to clarify such uncertainty.

Any enquiries or clarification requests concerning this Directive may be addressed to:

Head: National Payment System Department

South African Reserve Bank
P O Box 427
Pretoria
0001

They can also be emailed to npsdirectives@resbank.co.za.

Part 6: Annexures

Annexure A: Application to conduct a payment activity

1. A person seeking to conduct or provide a payment activity must:

1.1 apply to the Reserve Bank in the relevant form as set out in Annexure C; and

1.2 meet the following application requirements to the extent applicable and in respect of each payment activity.

2. General application requirements

2.1 **Incorporation.** The applicant must be a duly registered and/or an incorporated juristic person in the RSA.

2.2 **Supporting documentation.** The application must be in a form set out in Annexure C and accompanied by supporting information and documentation, which includes, although it is not limited to, the following:

2.2.1. **Incorporation and registration.** Certified copies of the notice of incorporation and registration certificate issued by the CIPC under the Companies Act.

2.2.2. **Memorandum of incorporation.** A certified copy of the memorandum of incorporation lodged with the CIPC.

2.2.3. **Address.** The address of the applicant's place of business and head office in the RSA. Where the applicant is incorporated outside of the RSA, the address of the applicant's headquarters or parent company/entity in addition to the address of their place of business and/or head office in the RSA.

2.2.4. **Business and operational plan.** A detailed business plan, including information on how the business model is funded, including own funds, loan funding (with the lender's name and domicile if applicable) and other sources

of funding, as well as detailed operational plan outlining the specific type of payment activity the applicant is applying for.

2.2.5. **Financial position.** Applicants currently operating must submit audited financial statements for the past three (3) financial years and a financial forecast for the next three (3) years. Applicants who have not yet commenced operations are required to submit a financial forecast for the next three (3) financial years.

2.2.6. **Compliance Officer.** The identity document and CV of the person responsible for the compliance function of a payment institution.

2.2.7. **Audit information.** Information and the identities of external auditors or firms, along with their names, addresses and contact details.

2.2.8. **Confirmations.** Confirmation whether the applicant and/or its parent company or parent company subsidiaries, where applicable:

a. were ever subject to an AML/CFT/CPF investigation;

b. were ever subject to any investigation by a local or international body, a regulatory authority, an enforcement agency or a court of law, and, if so, the applicant must provide details of such an investigation;

c. have ever been the subject of preventative, remedial or enforcement actions by any regulatory authority, and, if so, the applicant must provide details of the regulatory action taken;

d. have ever been denied authorisation, a licence or registration to perform a trade or conduct a business, or has such registration, authorisation or licence been revoked, withdrawn or terminated by a regulatory authority, and, if so, the applicant must provide details of denial of authorisation, licence or registration; and

e. have ever been or are currently regulated by a financial services regulatory authority, and, if so, they must provide the names of the regulatory authorities, regulated activities and periods of regulation.

3. Organisational structure

3.1 Details of the applicant's organisational structure must be provided, including, but not limited to, the following:

3.1.1 a description of the functions and responsibilities of each division, department or similar structure;

3.1.2 the number of staff employed per function and division or structure;

3.1.3 the full names and job title of key management staff responsible for operations related to payment activities;

3.1.4 reporting and communication lines with decision-making procedures and accountabilities;

3.1.5 the group structure if the applicant is a subsidiary of a group, indicating any shareholding or interest that the applicant may hold in other entities within the group, the name and registration number of such an entity, and a detailed description of the nature of the business activities in which the applicant holds such a shareholding or interest;

3.1.6 significant and beneficial owners as defined under section 1 of the FSR Act and FIC Act, and in accordance with the guidance notes issued by the Financial Intelligence Centre (FIC) or the Reserve Bank;

3.1.7 the equity and shareholding structure of the applicant, including the names, nationalities, country of incorporation, registration/identification/passport number and percentage of shareholding of each shareholder, significant owner and beneficial owner;

3.1.8 a declaration of source of funds by a significant shareholder;

3.1.9 copies of share certificates; and

3.1.10 a declaration from shareholders and ultimate beneficial owners that they hold the shares in their personal capacity, not as agents or nominees for disclosed or undisclosed persons, and that there are no silent partners controlling the shareholders of the legal entity.

4. Governance arrangements

4.1 The applicant must provide the following:

4.1.1 details of the applicant's governance arrangements, which have been approved by the governing body or highest level of authority, duly aligned with the prevailing best governance standards, principles, practices and internal control mechanisms;

4.1.2 a schematic view of the governing body, structures and subcommittees, which includes the constituents and chairpersonship, the composition of the management body and, if applicable, any other oversight body or committee, including its membership and anticipated establishment date (if not yet established);

4.1.3 a description of the group's governance arrangements, if applicable, where the applicant is a subsidiary; and

4.1.4 the identity, key duties and responsibilities as well as suitability assessment, including the competence, skills and payment-related experience, of the directors and key management personnel of the applicant.

4.2 The governing body shall be responsible for ensuring that a payment institution has an independent, permanent and effective compliance function to monitor and report on observance of all applicable laws, regulations and standards and on adherence by staff and members of the governing body to legal requirements,

proper codes of conduct and policy on conflicts of interest.

4.3 The payment institution shall have a governing body-approved compliance policy that is communicated to all staff, specifying the purpose, standing and authority of the compliance function within the payment institution.

4.4 Payment institutions must report transactions to the competent authority when there are suspicions, or reasonable grounds to suspect, that the proceeds are related to a crime or to the attempt or intention to use the funds or proceeds for the purpose of committing, concealing or benefitting from a crime.

5. Reporting requirements

5.1 By 28 February of each year, a payment institution must submit the following data for the period January to December of the preceding year:

5.1.1 the number of active clients in the past 12 months;

5.1.2 aggregated annual volumes and values per payment activity processed; and

5.1.3 aggregated annual amounts deposited in payment accounts for the various payment activities as well as an updated list of branches and agents, where applicable.

5.2 Banks are not required to report the above information regarding non-bank payment institutions that maintain segregated accounts with them

6. Fit-and-proper requirements

6.1 A payment institution must ensure that its directors and key persons are honest and have the necessary integrity, competence, skills and payment-related experience, certifications or training required to fulfil their roles and responsibilities, at application and on an ongoing basis.

6.2 The following indicates that a director or key person may lack honesty and integrity:

6.2.1 The person has been convicted (and that conviction has not been expunged) of a financial crime or is the subject of pending investigations or proceedings for such a crime.

6.2.2 The person has been convicted (and that conviction has not been expunged) or is the subject of pending investigations or proceedings which may lead to a conviction under any law in any jurisdiction, of an offence:

a. under a law relating to the regulation or supervision of a payment institution or a corresponding offence under the law of a foreign country involving theft, fraud, forgery, uttering a forged document, perjury or an offence involving dishonesty;
b. under the Prevention of Corruption Act, 1958 (Act No. 6 of 1958) or parts 1 to 4 or sections 17, 20 or 21 of the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004), POCDATARA, POCA or a corresponding offence under the law of a foreign country; or
c. where the penalty for the offence was, or may be, imprisonment or a significant fine.

6.2.3 The person has accepted civil liability or is civilly liable for theft, fraud, forgery, uttering a forged document, misrepresentation or dishonesty under any law.

6.2.4 The person has seriously or persistently failed to, or is failing to, manage any of his/her financial obligations (including debts) satisfactorily.

6.2.5 The person has been the subject of a civil judgment or will be the subject of any pending proceedings which may lead to such a judgment, in respect of an unpaid debt and which debt remains unpaid.

6.2.6 The person has been sequestrated or will be the subject of pending proceedings which may lead to sequestration under the Insolvency Act, 1936 (Act No. 23 of 1936) or a corresponding law of a foreign country and has not been rehabilitated in terms of that Act or law.

6.2.7 The person held a managerial position in an entity that underwent insolvency, business rescue or liquidation (or similar proceedings) because of their negligence/gross negligence.

6.2.8 The person has faced frequent or severe preventative, remedial or enforcement actions by a regulatory authority.

6.2.9 The person has breached fiduciary duties.

6.2.10 The person has been refused or has had any authorisation, licence or registration revoked to carry out a trade or business by a regulatory authority.

6.2.11 The person has been or is currently suspended, dismissed or disqualified from acting as a key person under any law.

6.2.12 The person has been refused or has had membership of any professional body revoked due to dishonesty, lack of integrity and/or business conduct issues.

6.2.13 The person has been disciplined, reprimanded, sanctioned, disqualified or removed by a professional body or a regulatory authority concerning honesty, integrity or business conduct.

6.2.14 The person has shown a lack of readiness and/or willingness to comply with legal, regulatory and/or professional standards.

6.2.15 The person has knowingly provided false or misleading information to a regulatory authority or has been uncooperative in dealings with them.

6.2.16 The person has been assessed and confirmed to be not fit and proper by a regulatory authority in previous assessments of fitness and propriety.

6.3 The payment institution must develop and maintain fitness and propriety policies and procedures that:

6.3.1 clearly define and document the fitness and propriety criteria required for directors and key persons, ensuring compliance with the fit-and-proper requirements

outlined in this Directive;

6.3.2 include periodic fit-and-proper assessments for key persons and directors;

6.3.3 ensure there is sufficient documentation retained for each fit-and-proper assessment to demonstrate the fitness and propriety of directors and key persons;

6.3.4 include processes to be applied in assessing whether a director or key person is fit and proper;

6.3.5 stipulate the steps and actions to be taken where the payment institution assesses an existing director or key person to no longer meet the fit-and-proper requirements, including where required by law, removal of the director/key person, and to notify the Reserve Bank of such an assessment and outcome as well as ensure the director/key person is removed (If the director or key person no longer meets the fit-and-proper requirements criteria and appropriate steps and actions are not taken or the director/key person is not removed, the Reserve Bank may revoke the authorisation.);

6.3.6 include adequate provisions for confidential reporting by any person who believes that a director or key person does not meet the payment institution's fit-and-proper criteria, and ensure the protection of such a person;

6.3.7 include requirements that directors or key persons consent to being subject to the fitness and propriety policy; and

6.3.8 include provisions that the payment institution consents to any former director or key person of the payment institution disclosing information to the Reserve Bank.

7. Risk management controls

7.1 The applicant must provide the following:

7.1.1 details of risk management measures, including a description of security controls and mitigation measures that will be taken to protect payers, payees and the NPS from risks such as cyber incidents, suspected fraud, fraud and the illegal use of

personal information; and

7.1.2 a detailed risk assessment of the payment activity it intends to offer. This should include an effective enterprise risk management framework to assess, identify, manage, mitigate, monitor and report any risks, including, but not limited to, any potential fraud risks and the security measures to mitigate them. Appropriate risk control measures to protect clients should also be outlined. The following should also be included:

a. a mapping of identified risks, including their types, assessment procedures and mitigation strategies;

b. scenarios analysis of possible risk events, including, but not limited to, high-severity operational risk events. This should consider the potential impact of failed or inadequate services arising from processes, systems, people or external events; and

c. a description of the information and communication technology (ICT) systems, which should include:

i. the ICT systems to be deployed;
ii. the architecture of the systems, including a network element diagram;
iii. the business ICT systems supporting the payment activity provided, such as the applicant's website, accounts/wallets, store of value, payment engine, risk and fraud management engine as well as client accounting;
iv. the support ICT systems used for the organisation and administration of the applicant, such as accounting, compliance reporting systems, staff management, client relationship management, email servers and internal file servers;
v. appropriate security policies and measures to safeguard the integrity, authenticity and confidentiality of data and operating processes, including transaction monitoring;
vi. information on whether those systems are already in use by the applicant or its group and the estimated date of implementation, if

applicable; and

vii. certification, where applicable, and compliance with internationally recognised best practice information security management standards.

7.2 On an ongoing basis, the applicant must conduct an annual assessment of the risk management framework, including annual testing of the ICT systems and a periodic assessment of the cybersecurity and cyber-resilience framework, third-party management plans and risk assessments.

7.3 The details of the applicant's cybersecurity and cyber-resilience policy, strategy and framework outlining the cybersecurity and cyber-resilience measures, processes, procedures and controls must comply with the applicable legislation and directives in respect of cybersecurity and cyber-resilience.

7.4 Security incidents management

7.4.1 The applicant must describe the procedures in place to monitor, manage and follow up on security incidents and client complaints related to security. This description should include:

a. organisational measures and tools for detecting, monitoring and preventing fraud;

b. details of the individuals and bodies responsible for assisting clients in cases of fraud, technical issues and claim management;

c. reporting lines for cases of fraud;

d. contact points for clients, including names and email addresses;

e. procedures for reporting incidents, including communications to internal or external bodies, with material cyber incidents being notified to the Reserve Bank;

f. the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks;

g. details of the procedures in place to monitor, manage and follow up on operational or security issues and incidents, including the cyber-related incidents reporting mechanism, sensitive payment data security measures and mitigation measures to comply with the cybersecurity and cyber-resilience regulatory framework issued by the Reserve Bank and operational or security-related client complaints;

h. information on the policies and processes used for collecting and sharing statistical data on performance, transactions and fraud/suspected fraud; and

i. information on an appropriate and tested technology system that enables interfacing with relevant systems to perform payment activities.

7.5 Business continuity management

7.5.1 The applicant must have robust business continuity capabilities and appropriate disaster recovery planning at the time of application. Applicants that are PSMB members are not required to provide the required information. The following information should be provided:

a. details of business continuity plans, including the identification of critical operations, effective contingency measures and procedures to regularly test and review the adequacy and effectiveness of these plans;

b. a business impact analysis outlining business processes and recovery objectives, recovery time objectives, recovery point objectives and protected assets;

c. the identification of back up sites, access to IT infrastructure as well as the key software and data needed to recover from a disaster or disruption;

d. an explanation of how the applicant will handle significant continuity events and disruptions, including the failure of key systems, loss of key data, inaccessibility of premises, national grid failure and the loss of key personnel;

e. the frequency of business continuity and disaster recovery plan testing, including how the results of these tests will be recorded and reviewed;

f. a description of the mitigation measures to be adopted in the event of termination of payment activities, ensuring the execution of pending payment transactions and the orderly termination of existing contracts; and

g. an estimate of the number and geographic locations of premises from which disaster recovery planning arrangements will be established.

7.6 For payment initiation, a payment initiation service provider must comply with the AML/CFT/CPF requirements in Annexure K.

8. Data protection

8.1. An applicant must:

8.1.1 provide details of how the confidentiality and integrity of payment data and systems will be protected, and whether the data is in transit or stored;

8.1.2 on an ongoing basis, conduct a formal review of its enterprise-wide information security risk assessment, at least annually. The institution must maintain ongoing action plans to address identified risks. In addition, detailed information security assessments must be conducted on identified high-risk areas, at least biannually;

8.1.3 ensure that appropriate protection and confidentiality arrangements are in place for data, information, systems and processes, in accordance with the POPI Act and other applicable data protection laws;

8.1.4 implement measures to ensure that the data and records maintained by a service provider or any third party remain the property of the applicant/payment institution;

8.1.5 in the event that the data and records are maintained by a third party or service provider that stores, processes, hosts, backs up, or otherwise holds or manages

such data and records on behalf of the payment institution, whether physically or electronically, as part of an outsourcing arrangement, provide their names and physical addresses;

8.1.6 develop and implement a framework for the retention of data and records of the payment institution;

8.1.7 where applicable, ensure compliance with data protection requirements of the PSMB, PCH system operators, settlement systems and designated settlement system operators;

8.1.8 take appropriate steps to mitigate loss of data, damage to and unauthorised destruction of data, unlawful access to or processing of personal information as well as data security risks, considering data sensitivity and how the data is transmitted, stored and encrypted; and

8.1.9 comply with applicable standards and practices for IT security as well as data and information security management systems to ensure cyber and data protection.

9. Safeguarding client funds

9.1 A payment institution must:

9.1.1 keep client funds separate from funds or assets belonging to it in a segregated account;

9.1.2 in its accounting records and financial statements, clearly indicate the client funds as being property belonging to a specified person for, or on whose behalf, the payment institution is acting, and properly identify the client funds in the books of the payment institution, in such a way as to show that it is an account which is held for the purpose of safeguarding client funds in accordance with this Directive; and

9.1.3 use the segregated account for holding those funds.

9.2 Despite anything to the contrary in any law or the common law, client funds held, kept in safe custody, controlled or administered by a payment institution under no

circumstances form part of the funds or assets of the payment institution, except where such funds are held in the formal beneficiary account with a bank, mutual bank, co-operative bank and branch of a foreign bank.

9.3 A payment institution may additionally cover client funds through an insurance policy or another comparable guarantee. It should be payable without delay if the payment institution is unable to meet its financial obligations, for an amount equal to what would have been segregated.

9.4 Where a payment institution holds client funds and is a designated settlement system participant that operates on a prefunded basis, the payment institution must transfer the funds held to its prefunded settlement account in the designated settlement system to fulfil settlement obligations. Once transferred into its designated settlement system participant's settlement prefunded account, such funds shall remain client funds. The designated settlement system participant must only transfer such funds to the payee designated settlement system participant's settlement account for onward payment to the payee.

9.5 Where the client funds are required to be transferred to the payee within a specified period after receipt of such funds, and where such funds are still held by the payer payment institution and not yet transferred/paid to the payee or payee payment institution by the end of the business day following the day when the funds have been received, such funds must be segregated and deposited in a segregated bank account.

9.6 Where a bank issues e-money, the bank must comply with the safeguarding client funds requirements set out in the above paragraphs. The bank must ensure that client funds are clearly segregated within its internal systems, ledgers and accounting records, so that the client funds are always clearly identifiable, ring-fenced and distinguishable from the bank's own funds and assets.

10. Accounting and audit

10.1 A payment institution must:

10.1.1 maintain accounting records on a continual basis and prepare financial statements that conform with the financial reporting standards prescribed under the Companies Act and any other generally accepted accounting practices;

10.1.2 have these records and annual financial statements audited by external auditors;

10.1.3 submit the audited financial statements to the Reserve Bank within four (4) months of the payment institution's financial year-end or within any extended period granted by the Reserve Bank; and

10.1.4 submit the information and identities of external auditors or firms, along with their names, addresses, the frequency of the audits and contact details.

10.2 Internal audit function

10.2.1 The governing body shall be responsible for ensuring that the payment institution has an independent, permanent and effective internal audit function commensurate with the size, nature of operations and complexity of its organisation.

10.2.2 The internal audit function shall provide independent assurance to the governing body and management on the quality and effectiveness of the payment institution's internal controls, risk management, compliance, corporate governance, and the systems and processes created by the business units, support functions and control functions.

10.2.3 The payment institution shall have an internal audit charter approved by the governing body's audit committee that articulates the purpose, standing and authority of the internal audit function within the payment institution.

11. Interest earned

11.1 Client funds held in a segregated account shall earn interest if the account is interest-bearing, and such interest shall accrue/belong to the payment institution that is holding client funds in such a segregated account.

11.2 As a result of interest earned, the payment institution must offer low-fee products

and services.

11.3 The clients of the payment institution shall not earn interest

12. Value date and availability of funds

12.1 A payment institution that holds the payment account of the payee and/or receives the payment instruction in favour of the payee must credit the payee's payment account:

12.1.1 within and in accordance with the clearing and settlement requirements and timelines as provided for in the NPS Act and directives, PCH agreements, settlement agreements, clearing and settlement rules, clearing and settlement operational procedures or relevant instrument(s) issued by the scheme manager, PSMB, the PCH system operators and operators of settlement systems, as the case may be; and

12.1.2 in the absence of the timelines as set out in 12.1.1, no later than two (2) business days on which a payment instruction is received or the amount/proceeds of the payment instruction are credited to the payee's payment institution's account, unless otherwise agreed to in writing between the payee and the payee's payment institution.

12.2 A payment institution shall ensure that payments or transactions from a payer's payment account are made in accordance with the payer's consent.

13. Prohibitions and restrictions

13.1 A payment institution, including a bank issuing e-money and the payment institution providing payment account types A and B of Group G, must not use client funds for any credit/lending or investment activities.

13.2 Any credit activities, including credit payment instruments, extension/facility or investment activities, shall be conducted using the payment institution's own funds, save for minimum capital and ongoing capital prescribed in this Directive, and

subject to the necessary authorisations being obtained from the relevant regulatory authorities.

14. Disclosure of charges

14.1 A payment institution must disclose all its fees and charges as well as any amendments, reasons and timing of such amendments in a clear, simple and understandable manner to its clients. In disclosing this information, the payment institution must consider the nature and complexity of the payment product and service as well as the assumed level of knowledge, understanding and experience of the targeted clients.

15. Agency arrangements

15.1 A payment institution may use an agent to conduct one or more payment activities, which the payment institution has been authorised to conduct by the Reserve Bank, on its behalf, subject to paragraph 15.2.

15.2 A payment institution that intends to use an agent must apply for and obtain the prior written approval of the Reserve Bank prior to appointing an agent, and must comply with the agency arrangements/requirements set out in Annexure F.

15.3 The payment institution is accountable and liable for the actions and omissions of its agents when those actions fall within the scope of the agency agreement.

15.4 Where the payment institution uses agents, the payment institution is required to ensure that the agents are listed on its website, outlets, branches and/or marketing platforms, such that they are visible or audible to the client.

15.5 An authorised payment institution providing third-party payments may appoint any person or another authorised payment institution providing third-party payments as agent, under governance of an agent agreement that must be compliant with the agency agreement requirements.

15.6 The payment institution appointed as an agent is prohibited from making use of the segregated account used by it as a principal for the provision of third-party

payments. A separate segregated account must be opened and maintained solely for the provision of agency business, on behalf of the authorised principal payment institution providing third-party payments.

16. Outsourcing arrangements

16.1 A payment institution that seeks to outsource its technology platform, internal audit and/or risk management functions as well as operational functions related to the provision of the payment activity under Annexure B, must apply for approval from the Reserve Bank in writing prior to the commencement of the outsourcing activities. This is also applicable in instances where a payment institution outsources from an entity forming part of the same group as the payment institution.

16.2 A payment institution shall not outsource an operational function if it is likely to materially impair the quality of its internal control as provided for in paragraph 17.3 or hinder the Reserve Bank's ability to monitor its compliance with this Directive.

16.3 An operational function is considered important if a defect or failure in its performance materially impairs:

16.3.1 the payment institution's continual compliance with this Directive; or

16.3.2 the financial performance, soundness or continuity of the payment institution's activities.

16.3.3 An outsourcing arrangement under this paragraph must comply with the following conditions: the senior management of the payment institution must retain accountability and must not delegate it;

16.3.4 the relationship and obligations of the payment institution towards its clients shall not be altered;

16.3.5 the outsourcing shall not amend, suspend or revoke a condition of the payment institution; and

16.3.6 any other conditions that the Reserve Bank may specify.

16.4 A payment institution must:

16.4.1 establish a service level agreement for all outsourcing arrangements; and

16.4.2 submit copies of it to the Reserve Bank within ten (10) business days of its signing.

16.5 A payment institution that engages in outsourcing arrangements must provide to the Reserve Bank:

16.5.1 a description of the manner in which the outsourced functions are monitored and controlled to avoid an impairment in the quality of its internal controls;

16.5.2 the identity of the persons that are responsible for each of the outsourced activities;

16.5.3 a clear description of the outsourced activities and their main characteristics;

16.5.4 confirmation that the outsourcing service provider has business continuity and disaster recovery plans in place that are regularly tested;

16.5.5 a copy of the draft outsourcing agreements; and

16.5.6 the off-site and on-site checks that it undertakes and their frequency, at least annually, as well as a description of the outsourcing arrangements.

17. Client complaints

17.1 A payment institution must, at application, provide:

17.1.1 a description of the structure and process for handling client complaints, including escalation procedures and service channels; and

17.1.2 details of the expected time frames for acknowledging, investigating and resolving client complaints.

Annexure B: Payment activities

1. Group A: Issuing of e-money and payment instruments

1.1. Category A1: Issuance of e-money

1.2. Category A2: Issuance of a payment instrument

2. Group B: Acquiring of payment instructions

3. Group C: Payment execution

3.1. Category C1: Payment execution

3.1.1. Clearing

3.1.2. Settlement

3.2. Category C2: Payment initiation

4. Group D: Payment to third persons/third-party payment providers

5. Group E: Schemes

6. Group F: Money remittance

7. Group G: Payment account A and B

Annexure C: Application form

Application form

Annexure D: Prudential requirements

1. For the purposes of this Directive, prudential requirements do not apply to banks regulated in terms of the Banks Act.

2. Minimum capital

2.1. Minimum capital serves as a regulatory safeguard to ensure that applicants have sound financial resources.

2.2. An applicant that is not classified as a bank under the Banks Act must, at the time of authorisation, hold minimum capital as indicated in the table below:

Payment activity	**Initial capital (R)**
Group A: Issuance of e-money and payment instruments 1. Category A1 a. Tier 1 e-money issuance b. Tier 2 e-money issuance 2. Category A2 c. Issuance of payment instruments	 a. R8 million b. R5 million c. Not applicable
Group B: Acquiring a. Acquiring payment instructions	 a. R3 million
Group C: Payment execution – clearing, settlement and payment initiation 1. Category C1 a. Clearing b. Settlement 2. Category C2 a. Payment initiation	 a. R1 million b. R3 million c. R2 million
Group D: Payments to third persons/parties a. Tier 1 TPPP b. Tier 2 TPPP	 a. R2 million b. R500 000
Group E: Schemes a. Schemes	 a. Not applicable
Group F: Money remittance a. Tier 1 money remittance b. Tier 2 money remittance	 a. R2 million b. R500 000

2.3. The minimum capital of a payment institution may consist of one or more of the following instruments:

2.3.1. common equity or shares (paid-in capital);

2.3.2. retained earnings;

2.3.3. accumulated comprehensive income; and/or

2.3.4. other reserves.

2.4. An applicant must provide evidence of minimum capital in accordance with its source of funding. If a payment institution is using paid-in capital, it must provide a bank statement, in the business' name, showing the monies being paid in. If the payment institution has already been operating and has sufficient reserves to meet the minimum capital requirement, it must provide a copy of the audited financial statements of the preceding year or interim financial statements.

2.4.1. If a payment institution offers two or more payment activities, the minimum capital is only the highest of the corresponding amounts.

2.5. Ongoing capital

2.5.1. Ongoing capital serves as a buffer to absorb unexpected losses that may arise and first losses when an entity is wound up.

2.5.2. A payment institution must consistently hold capital on an ongoing basis to absorb losses that it may incur as a going concern. Ongoing capital for the provision of payment activities in Group A must be a minimum of 2% of a payment institution's outstanding e-money liabilities calculated over a period of six (6) consecutive months. If a payment institution has not completed a full six (6) months' business by the date of the calculation, the requirement shall be a minimum of 2% of the projected outstanding e-money liabilities for the next six (6) consecutive months in its business plan. For payment activities in Group B to F (excluding Category C1 in Annexure D in respect of e-money), ongoing capital must be a minimum of 2%

of a payment institution's average payment values, calculated over a period of six (6) consecutive months. When calculating ongoing capital, there must be no double counting on payment values that reflect in more than one payment activity. If a payment institution has not completed a full six (6) months' business by the date of the calculation, the requirement shall be 2% of the projected average payment values for the next six (6) months in its business plan. Ongoing capital must make up 2% of a payment institution's average payment values, calculated over a period of six (6) months.

2.5.3. The ongoing capital held must not fall below the level of the minimum capital requirement for the payment activity provided. If 2% of the outstanding e-money liabilities or average payment values as stipulated in paragraph 2.5.2 is below the level of minimum capital, a payment institution's ongoing capital must be at least equal to the amount of minimum capital.

2.5.4. The ongoing capital of a payment institution may consist of the instruments listed in paragraph 2.3 above.

2.5.5. Ongoing capital must remain unencumbered and may not be ceded, pledged or used as collateral by the payment institution or any of its stakeholders.

2.5.6. If the payment institution is part of a group/conglomerate, it must ensure that its ongoing capital is segregated from the group's other activities or its subsidiaries.

2.5.7. The Reserve Bank reserves the right to impose higher ongoing requirements if it considers it essential to ensure that the payment institution can meet its regulatory obligations as outlined in this Directive.

2.5.8. A payment institution must annually provide the Reserve Bank with audited financial statements for the preceding 12-month period and confirm that its ongoing capital meets the stipulated requirements.

2.6. Financial soundness

2.6.1. An applicant that is not a bank as defined in the Banks Act and that has not been

operational must, at application, provide details of a reasonably measurable forecast budget calculation for the first three (3) financial years. This should show its ability to employ appropriate systems, resources and procedures to operate soundly. The details required include:

a. an income statement and balance sheet forecast, including target scenarios, stress scenarios and base assumptions, such as volume and value of transactions, number of clients/clients, pricing, average amount per transaction and expected profitability threshold;

b. explanations of the main lines of income and expenses, financial debts and the capital assets;

c. a diagram and detailed breakdown of the estimated cash flows and expenses for the next three (3) years; and

d. an overall forecast of the staff numbers for the next three (3) years.

2.6.2. An applicant that is already operating must provide a copy of the most recent financial statements or accounts to indicate that it operates its business in a sound manner.

2.6.3. The Reserve Bank settlement system operator must:

a. manage the liquidity risk caused by participants' financial or operational problems;

b. ensure participants have sufficient liquid resources through regular and rigorous stress-testing to effect settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios;

c. have clear procedures to report the stress-test results to its governing body and use these results to evaluate and adjust its liquidity risk management framework;

d. where it has prearranged funding arrangements, ensure that its participants have sufficient information to understand and manage liquidity risks;

e. use effective operational and analytical tools to measure, monitor and manage its liquidity risk continually and timely, including intraday liquidity. If the Reserve Bank settlement system operator maintains prefunding arrangements with participants and liquidity providers, it must also identify, measure and monitor its liquidity risk from these participants and liquidity providers;

f. ensure that participants hold sufficient liquid assets at all times to effect same-day settlement of payment obligations under various stress scenarios. Where appropriate, this must include intraday or multiday settlement. The stress scenarios must include a default of the participant and its affiliates that would result in the largest aggregate payment obligation under extreme but plausible market conditions. These assets must be held in the following manner:

   i. funds with the Reserve Bank; and/or

   ii. eligible collateral as defined in the Reserve Bank's collateral framework;

g. ensure that participants hold additional liquid resources for extreme but plausible market conditions in the ways defined in paragraph 2.6.3(f) or with a creditworthy financial institution in one or more of the following instruments:

   i. committed lines of credit;

   ii. committed foreign exchange swaps;

   iii. committed repos;

   iv. cash and assets with low credit, liquidity and market risks; and

   v. investments that are readily available and convertible into cash with prearranged and funding arrangements that are highly reliable, even in extreme but plausible market conditions;

h. have rules and procedures on settlement finality, consistent with the NPS Act provisions on settlement finality;

i. ensure final settlement by the end of the value date at a minimum; and

j. have rules on collateral management.

Annexure E: Transitional arrangements

A person that conducts a payment activity under Annexure B and is currently authorised, registered or designated in terms of the NPS Act, may continue conducting the payment activity during the transition period set out in this Annexure.

	Payment activity	**Transitional arrangements**
Group A: Issuing of e-money and payment instruments		
	Issuing of e-money (linked to Payment Account C)	**New:** All e-money issuers, whether a bank or non-bank, apply from the effective date of the Directive. **Current:** E-money issuers (including mobile money providers) operating in closed-loop payment systems (banks and non-banks) apply from the effective date of the Directive.
	Issuing of payment instrument	**New:** All issuers of payment instruments, whether a bank or non-bank, apply from the effective date of the Directive. **Current:** Issuers of payment instruments operating in closed-loop payment systems (banks and non-banks) apply from the effective date of the Directive.
Group B: Acquiring		
	Acquiring of payment instructions	**New:** Must apply from the effective date of the Directive. **Current:** Banks and non-banks must apply from the effective date of the Directive.
Group C: Payment execution (includes clearing and settlement) and payment initiation		
	Payment execution – clearing and settlement	**New:** Clearing or settlement system participants apply three (3) months after the effective date of the Directive. **Current:** Clearing or settlement system participants – within three (3) months from the effective date to apply.
	Payment initiation	**New:** Apply from the effective date of the Directive. **Current:** Continue with the registration requirements under Directive 2 of 2024 and apply from the effective date of the Directive.

Group D: TPPP/payments to third persons		
		New: Apply six (6) months after the effective date of the Directive. **Current:** Continue with the mandatory sponsorship and within six (6) months after the effective date, operate under the current regime and reapply six (6) months after the effective date of the Directive.
Group E: Schemes		
	Schemes	**Current and new:** New schemes (i.e. schemes established after the effective date of the Directive) are required to apply to the Reserve Bank for authorisation in accordance with this Directive. Current schemes (schemes already operational) must apply for authorisation from the effective date of the Directive. **Members** will be admitted by schemes, and the Reserve Bank will approve the entry, participation and exit criteria.
Group F: Money remittance		
	Money remittance	**New:** Apply six (6) months after the effective date of the Directive. **Current:** Existing money remitters that have partnered with banks or are authorised dealers with limited authority (ADLAs) or authorised dealers, and intend to offer domestic money remittance services, must apply four (4) months after the effective date of the Directive.
	Closed-loop payment systems	**New and existing:** Apply for registration six (6) months after the effective date of the Directive.

Agent

New: In respect of par 8.1 Annexure F, this prohibition shall apply to all new agreements entered into after the effective date of the Directive.

Current: Existing exclusivity agreements may remain in force for a transitional period not exceeding three (3) years, after which they must be terminated or amended to comply with this Directive. Payment institutions shall submit a compliance plan within 90 days of the effective date of the Directive.

Sponsorship

New: Apply six (6) months after the effective of the Directive.

Current: Continue with the sponsorship and within six (6) months after the publication operate under the current regime and reapply six (6) months after the effective date of the Directive.

All payment institutions that are conducting payment activities listed in Annexure B as at the publication date of this Directive may continue to conduct such activities for the duration of the transition period, if they comply with all applicable conditions, reporting requirements and any transitional arrangements prescribed by the Reserve Bank.

Annexure F: Use of agents

1. General

Where a payment institution intends to appoint an agent, it shall provide the following information to the Reserve Bank:

a. details of the legal and trading name of the agent;

b. physical or registered address of the agent;

c. where applicable, the registration, unique identification code or number of the agent;

d. a description of the internal control mechanisms that will be used by the agent to comply with the payment institution's obligations in relation to AML/CFT/CPF, to be updated without delay in the event of material changes;

e. the identity of directors and persons responsible for the management of the agent to be used in the provision of agency services and evidence that they meet fit-and-proper requirements as outlined in paragraph 28 of Annexure A;

f. agency services to be provided through the agent;

g. the proposed geographical coverage of the agent over a three-year period;

h. the due diligence policy and procedures conducted on the agent and the payment institution's due diligence report on the agent;

i. the IT systems, processes and infrastructure that are used by the agents to perform activities on behalf of the payment institution;

j. the selection policy, monitoring procedures and agents' training;

k. copies of all draft agency agreements;

l. a risk assessment report of the operations to be performed through the agent, including the mitigating measures to be adopted to control the identified risks;

m. an internal audit report regarding internal controls to be used for agency business and for any master agent;

n. the AML/CFT/CPF policies and procedures as they relate to agency business, including Know Your Customer (KYC) procedures, if applicable;

o. the operational policies and procedures of the payment institution, including those relating to monitoring and enforcing compliance of agents and master agents with all requirements under this Directive;

p. a policy document on how the payment institution will address the risk of the agent overselling or overcharging; and

q. the full incentive structure for an agent and master agent associated with every service provided, including the agent fee and revenue-sharing structure.

2. Information verification by the Reserve Bank

a. Prior to the Reserve Bank approving the agent, the Reserve Bank shall, if it considers that the information provided to it is incorrect, take further action to verify the information.

3. Requirements of agency agreement

3.1 An agency agreement shall, at a minimum:

a. define the rights and responsibilities of both parties (i.e. agent and payment institution);

b. set the scope of work to be performed by the agent and specify that the

payment institution is responsible and liable for the actions or omissions of an agent performing the services on its behalf, even if the action has not been authorised in the agreement but relates to the agency business;

c. specify the actions that are permissible;

d. specify that the agents who render an agency service in respect of outward payments shall operate against prefunded accounts only;

e. set the agent and master agent remuneration and any revenue-sharing structure, including incentives and bonuses;

f. state that any outsourced service is subject to prior written regulatory approval by the Reserve Bank;

g. state that an agent shall not perform management functions, make management decisions, or act or purport to act on behalf of management or as an employee of the payment institution;

h. state that an agent, master agent or an employee of an agent or master agent has no claim to be treated as an employee of the payment institution;

i. specify that the agent shall ensure the safe-keeping of all relevant records not already captured on the platform and ensure that the records are, at regular prespecified intervals, moved to the payment institution who shall ensure the safe-keeping of these records for at least five (5) years;

j. state that records and data relating to a client of the payment institution and the transactions that are collected or generated by the agent or master agent, whether from the clients, payment institution or other sources, are the sole property of the payment institution and shall be kept confidential;

k. state that the agent or master agent is bound to complete confidentiality agreements regarding the clients and their transactions;

l. state the management of conflicts of interest between the agent or master agent and the payment institution where the agent or master agent has entered into agency arrangements with multiple independent payment institutions.

m. allow unrestricted access to the Reserve Bank in respect of all internal systems, information, data and documents of the agent or master agent relating to the agency business;

n. stipulate that an agent or master agent may not subcontract its contractual obligations to a third party without the payment institution's prior written consent and the Reserve Bank's approval; and

o. establish a protocol for changing the terms of the service contract, stipulations for default and termination of the contract as well as for dispute resolution.

4. Responsibilities of the payment institution and master agent

4.1 A payment institution or master agent shall:

a. define a contingency plan to mitigate any significant disruption, discontinuity or gap in the agency services;

b. prohibit an agent from charging any additional fee to clients for services rendered by the agent on behalf of the payment institution beyond the fees prescribed and advertised by the payment institution;

c. conduct adequate compulsory onboarding and ongoing training of agents, and ensure that agents are well trained to offer knowledgeable support to clients; and

d. conduct regular monitoring of an agent to ensure that the services provided by the agent are safe and reliable and that they meet the requirements of this Directive.

5. Agent eligibility and due diligence

5.1 The payment institution shall consider the following information in assessing the eligibility of a prospective agent or master agent:

a. criminal record in matters relating to finance, fraud, honesty or integrity;

b. negative information in credit bureaus;

c. business experience and track record, where applicable;

d. the prospective master agent shall demonstrate financial soundness and cash-handling capabilities, arrangements for security and internal control in respect of operational risks; and

e. any other relevant matter.

5.2 A payment institution shall have clear and well-documented policies and procedures in place for conducting due diligence on agents and prospective agents. The procedures shall, at a minimum, include:

a. new agent take-on procedures;

b. initial due diligence as well as regular due diligence checks to be performed at specified intervals; and

c. a list of early warning signals and corrective actions.

5.3 An agent due diligence shall clearly specify the roles and responsibilities of various functions and individuals within the business of the payment institution regarding the management and supervision of the agent.

6. Appointment of a master agent

6.1 A payment institution shall, on an ongoing basis, provide the Reserve Bank with

the following information in respect of the master agent within thirty (30) days of the appointment of the master agent, but prior to using the master agent services:

a. information about the master agent and the organisational structure of the master agent, including the name, identification and business registration number of the agents under the master agent;

b. the physical location, global positioning system co-ordinates, postal address, email address and telephone number of the head office and any other offices or agent points;

c. a description of the commercial activities of the master agent for the past twelve
(12) months before the date of the application;

d. a copy of the agency agreement stating any variation in the terms and conditions from the standard agency agreement and assigning reasons for any variations;

e. the due diligence policy in respect of the master agent and new agent take-on procedures;

f. a copy of the standard agency agreement under which the master agent contracts an agent on behalf of the payment institution;

g. an internal audit report by the payment institution regarding the internal controls of the master agent in relation to the agency business;

h. AML/CFT/CPF policies and procedures of the master agent as the policies and procedures relate to agency business, including KYC procedures;

i. agent operational policies and procedures, including those in respect of monitoring and enforcing compliance by agents with all requirements under this Directive;

j. the agency service to be provided by the master agent and the transaction limits;

k. the incentive structure for the agent, managed by the master agent, associated with the service, agent fee and revenue-sharing structure; and

l. any other information that the Reserve Bank may require.

7. Appointment of an agent

7.1 A payment institution shall, on an ongoing basis, provide the Reserve Bank with the following information about an agent within thirty (30) days of the appointment of the agent, but prior to using the agent's service:

a. information about the agent and the business organisation of the agent, including the names of all persons and their identification or business registration numbers;

b. the physical location, global positioning system co-ordinates, email address and telephone number;

c. a description of the commercial activities of agent for the past twelve (12) months before the date of the application;

d. a copy of the agency agreement stating any variation in the terms and conditions from the standard agency agreement and assigning reasons for any variations;

e. the payment activity to be provided by the agent and the transaction limits;

f. the incentive structure for the agent, managed by the master agent, associated with the service, agent fee and revenue-sharing structure; and

g. any other information that the Reserve Bank may require.

8. Exclusivity agency agreement

8.1 A payment institution shall not sign an exclusive agreement with an agent/master agent.

8.2 An agent/master agent may enter into an agreement with more than one payment institution.

9. Termination of agency agreement

9.1 A payment institution shall terminate an agent agreement and relationship where the agent:

a. is convicted of an offence involving:
   i. fraud;
   ii. dishonesty; and/or
   iii. other financial impropriety;

b. as a juristic person, is being dissolved, wound up or declared insolvent by a court;

c. as a sole proprietor, dies or becomes mentally incapacitated;

d. transfers, relocates or ceases operating at the place of business without the prior written consent of the payment institution;

e. contravenes any provision of the NPS Act or this Directive; or

f. introduces unacceptable levels of risk in terms of the payment institution's risk management framework.

9.2 Where an agency agreement is terminated, the payment institution shall:

a. publish a notice of the termination in the area/location where the agent operates; and

b. inform the Reserve Bank of the termination within ten (10) business days.

9.3 The payment institution shall, on an ongoing basis, obtain the prior written approval from the Reserve Bank to use agents.

10. Publication of agents/master agents

10.1. A payment institution must make available and publish, on its company website, a list of all the agents and master agents that it will use, and ensure that the following information is included:

a. the name and physical location; and

b. which agents are affiliated with a particular master agent.

11. Notification of changes

11.1. A payment institution that intends to introduce a material change in the services of an agent shall obtain the prior written approval of the Reserve Bank.

Annexure G: Payment activity limits

Payment activity	Tier	Transaction limits	Balance limits (at any given time)
1. E-money issuance	**Tier 1 (large scale):** > R5 million average monthly transaction values	**Natural persons:** Per day: R15 000 Per month: R50 000 **Juristic persons:** Per month: R250 000	**Natural persons:** R50 000 **Juristic persons:** R100 000
	Tier 2 (small scale): < R5 million average monthly transaction values	**Natural persons:** Per day: R5 000 Per month: R20 000 **Juristic persons:** Per month: R100 000	**Natural persons:** R20 000 **Juristic persons:** R50 000
2. Money remittance	**Tier 1 (large scale):** > R5 million average monthly transaction values	**Natural persons:** Per day: R5 000 Per month: R50 000	**Natural persons:** R50 000
	Tier 2 (small scale): < R5 million average monthly transaction values	**Natural persons:** Per day: R2 500 Per month: R25 000	**Natural persons:** R25 000
3. Third-party payment provider	> R5 million average monthly transaction values	N/A	N/A
	Tier 2 (small scale): < R5 million average monthly transaction values	N/A	N/A

Annexure H: Fit-and-proper declaration

[insert text for Annexure H]

Annexure I: Linkages of payment activities

Payment activity	Key dependencies	Scheme	Clearing	Settlement
Issuance of e-money (Payment Account C)	**Mandatory:** Issuance of payment instrument	Must be a member of a PSMB and participate in the relevant PCHs/scheme or can be sponsored	Must be a clearing system participant or appoint one (can be sponsored)	Must be a settlement system participant or appoint one (can be sponsored)
Issuance of a payment instrument	**Mandatory:** Payment Account – Issuance of e-money, Payment Account A or B)	Must be member of a scheme	n/a	n/a
Acquiring of payment instructions	**Optional:** Non-banks: Issuance of e-money (Payment Account C)	Must be a member of a PSMB and participate in the relevant PCHs/scheme	Must be a clearing system participant or appoint one (can be sponsored)	Must be a settlement system participant or appoint one (can be sponsored)
Payment initiation	n/a	n/a	n/a	n/a
Payment to third persons/third-party payment providers	n/a		n/a	n/a
Money remittance	**Optional:** Payment Account – Issuance of e-money, Payment Account A or B)	Must be a member of a PSMB and participate in the relevant PCHs/scheme or can be sponsored	Must be a clearing system participant or appoint one (can be sponsored)	Must be a settlement system participant or appoint one (can be sponsored)

Annexure J: Directives and position papers that will be repealed by this directive

1. Directive for conduct within the national payment system in respect of payments to third persons – Directive No. 1 of 2007

2. Directive in respect of issuing of electronic funds transfer credit payment instructions on behalf of the payer in the national payment system – Directive No. 2 of 2024

3. Position Paper on Electronic Money – Position Paper No. 1 of 2009

Annexure K: Anti-Money Laundering, Counter-Terrorism Financing and Counter-Proliferation Financing requirements

1. Anti-money laundering, counter-terrorism financing and counter-proliferation financing (AML/CFT/CPF)

Payment institutions that are accountable institutions in terms of the FIC Act are required to adhere to the requirements below.

1.1 Payment institutions that are accountable institutions in terms of the FIC Act must:

1.1.1 comply with the provisions of chapter 3 of the FIC Act relating to customer due diligence;

1.1.2 comply with all the provisions in the FIC Act and the regulations, directives, guidance notes and public compliance communications issued in terms of the FIC Act;

1.1.3 have in place adequate human, financial, technical and other resources to ensure compliance with the provisions of the FIC Act;

1.1.4 comply with the provisions of POCDATARA relating to AML/CFT/CPF; and

1.1.5 comply with the provisions of POCA relating to AML/CFT/CPF;

1.2 The Reserve Bank may require the submission of AML/CFT/CPF risk controls and measures at any time and may conduct on-site and/or off-site inspections to assess compliance with the FIC Act, POCA and POCDATARA.

1.3 The Reserve Bank shall notify a payment institution of any non-compliance identified during an on-site or an off-site inspection and provide for a period of thirty (30) days for the payment institution to remedy the identified non-compliance.

1.4 The payment institution must establish and maintain effective policies, procedures and controls to ensure the timely reporting of unusual and/or suspicious transactions by staff to the FIC.

2. AML/CFT/CPF requirements for payment institutions that are not accountable institutions

Payment institutions that are not accountable institutions in terms of the FIC Act must, as an authorisation requirement, adhere to the following AML/CFT/CPF requirements.

2.1 Payment institutions must adhere to the due diligence requirements below.

2.1.1 A payment institution may not establish a business relationship or conclude a transaction with a client:

a. on which they have not conducted due diligence;
b. they cannot identify; or
c. that appears to be using a false or fictitious identity.

2.1.2 When a payment institution engages with a prospective client for purposes of performing a once-off payment activity or to establish an ongoing business relationship to provide a payment activity, it must ensure that it has internal risk and compliance processes, which provide for a payment institution to conduct due diligence on prospective clients as follows:

a. identify and verify the identity of the client;
b. where the client of a payment institution is acting on behalf of another person, the payment institution must be able to identify and verify:
    i. the identity of that other person; and
    ii. the client's authority to act on behalf of that person.

2.1.3 Where another person is acting on behalf of a payment institution's client, the payment institution must identify and verify:

a. the identity of that person; and
b. that person's authority to act on behalf of the client.

2.1.4 Where a client of a payment institution is a legal person or a natural person acting on behalf of a partnership, trust or similar arrangement between natural persons, the payment institution must, in addition to the requirements in paragraphs 2.1.1 to 2.1.3, determine the following:

a. the nature of the client's activities; and

b. the client's ownership and control structure, by identifying the shareholders and the significant shareholder or beneficial owner of the client.

2.1.5 Where the client of a payment institution is a legal person the payment must, in addition to the requirements in paragraphs 2.1.1 to 2.1.4 and in accordance with its Risk Management and Compliance Programme,

a. Establish the identity of the beneficial owner of the client by

i. determining the identity of each natural person who, independently or together with another person, has controlling ownership interest in the legal person;

ii. if in doubt whether a natural person contemplated in subparagraph (i) is the beneficial owner of the legal person or no natural person has a controlling ownership interest in the legal person, determining the identity of each natural person who exercises control of that legal person through other means, including his or her own ownership or control of other legal persons, partnerships or trust; or

iii. if a natural person is not identified as contemplated in subparagraph (ii), determining the identity of each natural person who exercises control over the management of the legal person, including in his or her capacity as executive officer, non-executive director, independent non-executive director, director or manager; and

b. take reasonable steps to verify the identity of the beneficial owner of the client, so that the accountable institution is satisfied that it knows who the beneficial owner is

2.1.6 Where a payment institution enters a single transaction or establishes a business relationship with a person acting on behalf of a partnership, the payment institution must, in addition to the requirements in paragraphs 2.1.1 to 2.1.5 and in accordance with its Risk Management and Compliance Programme

a. establish the identifying name of the partnership, if applicable;

b. establish the identity of,

   i. every partner, including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership

   ii. if a partner in the partnership is a legal person or natural person acting on behalf of a partnership or in pursuance of the provisions of a trust agreement, the beneficial owner of that legal person, partnership or trust;

   iii. the natural person who exercises executive control over the partnership; and

   iv. each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the payment institution on behalf of the partnership.

c. take reasonable steps to verify,

   i. the particulars obtained in paragraph 2.2.6 (a); and

   ii. the identities of the natural persons referred to in paragraph 2.1.6 (b) so that the payment institution is satisfied that it knows the identities of the natural persons concerned.

2.1.7 Where a payment institution enters a single transaction or establishes a business relationship with a person acting on behalf of a partnership, the payment institution must, in addition to the requirements in paragraphs 2.1.1 to 2.1.5 and in accordance with its Risk Management and Compliance Programme

a. establish the identifying name and number of the trust, if applicable;

b. establish the address of the Master of the High Court where the trust is registered, if applicable

c. in respect of the founder of the trust, establish the identity of,

   i. each founder; and

   ii. if a founder of the trust is a legal person or a person acting on behalf of a partnership or in pursuance of the provisions of a trust agreement, the beneficial owner of that legal person, partnership or trust;

d. in respect of the trustees of that trust, establish the identity of,

   i. each trustee and if a trustee is a legal person or a person acting on behalf of a partnership, the beneficial owner of that legal person or partnership; and

   ii. each natural person who purports to be authorised to enter into a single transaction or establish a business relationship with the payment institution on

behalf of the trust, whether such a person is appointed as a trustee of the trust or not;

e. in respect of the beneficiaries of a trust, establish

i. the identity of each beneficiary referred to by name in the trust instrument or other founding instrument in terms of which the trust is created and where a beneficiary referred to by name in the trust instrument is a legal person or a person acting on behalf of a partnership or in pursuance of the provisions of a trust agreement, the beneficial owner of that legal person, person or trust; and

ii. if beneficiaries are not referred to by name in the trust instrument or other founding instrument in terms of which the trust is created, the particulars of how the beneficiaries of the trust are determined

f. take reasonable steps to verify the particulars obtained in paragraphs 2.1.7 (a), (b) and (e)(ii)

g. take reasonable steps to verify the identities of the natural persons referred to in paragraphs 2.1.7 (c), (d) and (e)(i) so that the payment institution is satisfied that it knows the identities of the natural persons concerned

2.1.8 A payment institution must ensure that it takes reasonable steps to identify and verify the identity of all its clients, as required in the paragraphs above.

2.1.9 A payment institution must ensure that, in addition to conducting due diligence prior to performing a one-off payment activity or establishing an ongoing business relationship to provide a payment activity, its internal risk and compliance processes make provisions for conducting ongoing due diligence on its clients.

2.1.10 Ongoing due diligence must be carried out for the duration of the business relationship.

2.1.11 A payment institution must ensure that ongoing due diligence provides for the following:

a. ensures that a client's identification and verification information remains current and accurate;

b. monitors a client's transactions to ensure that they are consistent with the payment institution's knowledge of the client; and

c. monitors a client's transactions for any unusual or suspicious transactions. Where unusual or suspicious transactions are identified, such transactions must be reported to the Financial Intelligence Centre in accordance with section 29 of the FIC Act.

2.1.12 Where a payment institution is unable to conduct due diligence on a client, as required in paragraphs 2.1.1 to 2.1.7, the payment institution may not establish a business relationship to conduct a payment activity with the client or conclude a once-off payment activity for the client.

2.1.13 Where a payment institution is unable to conduct ongoing due diligence on a client, it must:

a. suspend the business relationship until such a time that they can conduct ongoing due diligence; or

b. terminate the business relationship.

2.1.14 A payment institution must apply enhanced due diligence measures in accordance with its Risk Management and Compliance Programme in respect of the following

a. politically exposed persons;

b. correspondent relationships; and

c. complex or unusually large transactions;

2.1.15 Enhanced due diligence measures may include,

a. Obtaining additional identification information;

b. Obtaining information on source of funds or source of wealth;

c. obtaining senior management approval before entering into a business relationship or conducting a transaction with a client;

d. increasing the degree and frequency of transaction monitoring; and

2.2. A payment institution must,

2.2.1. develop and maintain a Risk Management and Compliance Programme that follows a risk-based approach and includes,

b. internal policies, procedures and controls that a payment institution has in place to ensure compliance with paragraph 2 of Annexure K.

c. customer due diligence procedures

d. transaction monitoring procedures

e. suspicious transaction reporting procedures

f. sanction screening controls

g. staff training measures

h. record-keeping procedures

2.2.2. identify, assess, document and understand its ML/TF/PF risks to which it is exposed and shall consider,

a. client risk,

b. activity and product risk,

c. delivery channel risk,

d. geographic risk, and

e. transaction risk.

2.2.3. appoint a competent Compliance Officer that will be responsible for implementing and monitoring AML/CFT/CPF policies, procedures and controls and for reporting to the FIC.

2.2.4. ensure that all records, physical and electronic, pertaining to a business relationship or transactions with a client, including once-off transactions, are kept for at least five (5) years from the date of termination of a business relationship or when a transaction is concluded. The records to be kept include, but not limited to the following;

i. customer due diligence records;

j. the nature of the business relationship or transaction including the amounts involved and parties to a transaction;

k. any document or copy of a document or copy of a document obtained by a payment institution to verify a client's identity;

l. the records that a payment institution keeps with a third party.

2.2.5. conduct transaction monitoring and reporting of suspicious and unusual transactions to the FIC, in terms of section 29 of the FIC Act.

2.2.6. screen clients against applicable sanctions lists and report matches to the FIC.

2.2.7. conduct training of staff on AML/CFT/CPF requirements as contained in paragraph 2 of Annexure K, including the contents of its Risk Management and Compliance Programme.

2.2.8. comply with provisions of POCDATARA relating to AML/CFT/CPF

2.2.9. comply with the provisions of POCA relating to AML/CFT/CPF

2.3. A payment institution must implement, maintain and evidence a robust AML/CFT/CPF compliance framework aligned with any directives or notices issued by the Reserve Bank and competent authorities.

2.4. A payment institution must ensure that it has adequate human, financial, technical and other resources to ensure compliance with paragraph 2 of Annexure K.

2.5. The Reserve Bank may require the submission of a payment institutions risk management and compliance programme at any time and may conduct on-site and/or off-site inspections to assess compliance with paragraph 2 of Annexure K, POCA and POCDATARA.

2.6. The Reserve Bank shall notify a payment institution of any non-compliance identified during an on-site or an off-site inspection and provide for a period of thirty (30) days for the payment institution to remedy the identified non-compliance.