South African Reserve Bank

National Payment System Department

Draft for consultation

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

Directive X of 2025

November 2025

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 important for the safe and efficient functioning of the economy. Robust authorisation requirements are thus critical, and generally more intense for inner core activities such as payment account services, which

demand a higher level of regulatory scrutiny. Applicants are expected to undertake thorough due diligence and submit well-prepared applications that demonstrate their capacity to meet the applicable requirements set out in this Directive.

1.5 This Directive stipulates the requirements with which any person (bank or non-bank) must comply should they wish to offer/conduct specific payment activities, as listed in Annexure B, including those offered/conducted in a closed-loop payment system. These activities, outlined in Annexure B, include those exempted from the definition of 'the business of a bank' in terms of the Banks Act, 1990 (Act No. 94 of 1990), as amended (Banks Act), as contemplated by Notice XX of 2025 (Exemption Notice), as well as those that are not exempt in the Exemption Notice. Furthermore, the additional purpose of this Directive is outlined 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 service provided by a payment institution contracting with a payee to accept and process payment instructions, which results in a transfer of funds to the payee.

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 the 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 person who accepts money or proceeds of payment instructions, as a regular feature of that person’s business activity, from multiple payers on behalf of a beneficiary.

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

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

3.12 **‘Client’** means a person to whom or for whom a payment activity is offered or provided, in whatever capacity, and includes a successor in title of such person.

3.13 **‘Client funds’** means any funds held, kept in safe custody, controlled, administered or alienated by a payment institution in trust for, or on behalf of, a client when conducting or providing payment activities listed in Annexure B.

3.14 **‘Client-consented data’** means client data held by a payment institution, including client transactions, personal identification data and client financial history, that 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.

3.15 **‘Closed-loop payment system or payment activity’** means a payment system or payment activity 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, excluding:

a. on-us transactions that are in the open-loop payment system where both the payer and the payee are clients of the same entity; and
b. gift cards, mall and airtime vouchers, loyalty programmes, prepaid cards or instruments issued solely for the purchase of goods and services from the issuing entity and which are not redeemable for cash.

3.16 **‘Control function’** means each of the following:

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

3.17 **'Designation'** means the designation by the Reserve Bank of a clearing system participant, in terms of section 6(3)(a) of the NPS Act, to clear payment instructions.

3.18 **'Exemption Notice'** means Notice XX of 2025 issued in terms of paragraph (cc) of the definition of 'the business of a bank' in section 1(1) of the Banks Act.

3.19 **'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 issuer; and (iii) can be redeemed at face value on demand. E-money may be accepted as a means of payment by persons other than the issuer or be accepted within the issuer's network or ecosystem. For the purposes of this Directive, e-money includes 'mobile money'.

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

3.21 **'Face value'** means the e-money amount equivalent to the fiat value.

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

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

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

3.25 **‘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.

3.26 **‘Informed consent’** means any voluntary, specific and informed expression of will in terms of which consent is given by the payer for the processing of the payer’s information for purposes of payment initiation.

3.27 ‘**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.

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

3.29 **‘Issuing of payment instruments’** means the provision of clients with payment instruments that allow clients to make a payment or transfer funds electronically.

3.30 **‘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 in charge of 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 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; and
f. the head of a function of the payment institution that this Directive requires to be performed.

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

3.32 **'Mobile money'** means e-money where an electronic wallet service allows users to store, send and receive money using their mobile phone.

3.33 **'Money remitter'** means a person performing 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.

3.34 **'Outsourcing arrangement'** means an arrangement between a payment institution and another person for the provision of, or for the payment institution of 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.

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

3.36 **'Payer'** means a natural or juristic person who holds a payment account and allows a payment instruction in respect of client funds from that payment account, or, where there is no payment account, a person who gives a payment instruction regarding client funds.

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

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

3.39 **'Payment account'** means an account or store of value that is used for the transfer of funds. It refers to a Payment Account A, Payment Account B in Annexure B, Group G and Payment Account C, which is an e-money account in Annexure B, Group A1.

3.40 **'Payment account service provider'** means a payment service provider providing and maintaining a payment account for a payer.

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

3.42 **'Payment execution'** means the ability of a payment institution to submit clearing and settlement instructions or to process payment instructions for the purposes of clearing or settlement.

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

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

3.45 **'Payment institution'** means a person that is authorised and/or designated and/or registered and/or exempted where applicable in terms of the Exemption Notice or this Directive, and regulated under the NPS Act and this Directive to perform a payment activity listed in Annexure B.

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

3.47 **'Payment instrument'** means a tool or mechanism, physical or electronic, which enables or initiates the transfer of funds from a payer to a payee to make or receive a payment.

3.48 **'Payment system'** as defined in the NPS Act; it includes a closed-loop payment system or an interoperable payment system.

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

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

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

3.52 **‘POPI Act’** means the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

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

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

3.55 **‘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 instrument.

3.56 **‘Sensitive payment data’** means data, including personalised security credentials, which can be used to commit fraud. For the activities of payment initiation service providers, the name of the account owner and the account number do not constitute sensitive payment data.

3.57 **‘Settlement’** as defined in the NPS Act.

3.58 **‘Settlement system participant’** as defined in the NPS Act.

3.59 **‘Simple due diligence’** means where a payment institution has systems and controls in place that may allow for:

a. less information to be obtained from customers and potential customers when conducting their customer due diligence;
b. less secure confirmation of information to be applied; and
c. less frequent scrutiny to be conducted where the assessed risk of a customer or potential customer is low.

3.60 **‘Store of value’** means funds stored in a facility provided by a bank or non-bank.

3.61 **‘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.

3.62 **‘Third-party payment’** means the acceptance of money or payment instructions by third-party providers as a regular feature of business, from any other person, for the purposes of making payment on behalf of that other person to a third party to whom that payment is due.

3.63 **‘Third-party payment provider’ (TPPP)** means a person that provides third-party payment. A TPPP may be a payer service provider and/or a beneficiary service provider as defined in 3.37 and 3.9 above respectively.

3.64 **‘Trust account’** means a legally protected bank account in which a payment institution holds client funds in trust, segregated/separated from its own operational funds, to safeguard those funds from the payment institution’s insolvency or misuse.

3.65 **‘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, 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 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;

4.3.2 authorisation of payment clearing house (PCH) system operators;

4.3.3 authorisation to provide Payment Account A and Payment Account B, as outlined in Annexure B, Group G (This authorisation remains the responsibility of the Prudential Authority and National Credit Regulator respectively, 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

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 generally not required to comply with this Directive, except where specifically indicated/stated.

Part 2: Purpose, position, exemptions and sponsorships

5. Purpose

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 restricted from holding client funds in the absence of a sponsorship arrangement with a licensed bank or a third-party payment provider (TPPP) registration, where payment is due. This activity-based regulatory framework enables any authorised payment institution, including non-banks, to offer payment activities listed in Annexure B, provided they meet the applicable authorisation 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 activities;
5.2.4 requirements for settlement system operators;
5.2.5 requirements for payment account service providers in respect of payment activity C2 (payment initiation);
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 listed 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 and 20.

6.4 Any person that provides a closed-loop payment system or payment activity listed in paragraph 45.4 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. However, 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 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 activity involving acceptance of deposits or the soliciting 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' under the Banks Act. Such activities will remain subject to the Banks Act. Therefore, non-banks conducting these activities must either obtain a banking licence or have a business relationship with a bank. Any non-bank offering such payment activities without being registered as a bank or having a business relationship with a bank will be contravening the Banks Act.

6.7 The Reserve Bank retains the discretion to decline any application for authorisation or designation or registration that does not comply with the requirements stipulated in this Directive**.** Applicants whose applications have been declined may submit a new application no earlier than ninety (90) 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 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 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.

7. Exemptions

7.1 The Reserve Bank may, upon application or at its own discretion, exempt any person 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 any existing legislation also regulates a payment activity; or

7.1.3 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 in respect of prudential requirements only after consulting and obtaining written agreement from the Prudential Authority and subject to any additional conditions set by the Prudential Authority or the Reserve Bank.

7.3 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.

7.4 An exemption granted under paragraph 7 may be provided for a specified period and subject to conditions as prescribed by the Reserve Bank and the Prudential Authority in respect of prudential requirements.

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

7.6 An exemption may be withdrawn in its entirety or in part on any grounds which the Reserve Bank, or where applicable the Prudential Authority, may consider justifiable.

7.7 The Reserve Bank may suspend or withdraw the exemption in the event of non-compliance with the stipulated conditions.

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

7.9 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:

7.9.1 general application: paragraph 2 of Annexure A;
7.9.2 organisational structure: paragraph 3 of Annexure A;
7.9.3 governance: paragraph 4 of Annexure A;
7.9.4 fit-and-proper requirements: paragraph 6 of Annexure A;
7.9.5 prudential requirements: Annexure D;
7.9.6 safeguarding client funds: paragraph 9 of Annexure A;
7.9.7 agency arrangements: paragraph 16 of Annexure A; and
7.9.8 outsourcing arrangements: paragraph 17 of Annexure A.

7.10 Persons registered as banks under the Banks Act must comply with reporting, risk management, 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 offered/conducted by a bank.

7.11 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 requirements; fit-and-proper requirements; prudential requirements; and accounting.

8. Sponsorships

8.1 The Reserve Bank may, upon application and at its discretion, approve indirect access of an applicant to the NPS, 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 volumes and values fall below

the prescribed threshold outlined in paragraph 42.6, may operate under a sponsorship arrangement with an authorised or designated payment institution or obtain registration in accordance with Part 3 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, 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, PSMB 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 and the PSMB.

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

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

8.1.7 The sponsoring payment institution and sponsored payment institution must provide prior written notice to the Reserve Bank of the sponsorship arrangement, demonstrating compliance with the sponsorship requirements prescribed by the Reserve Bank and the PSMB, 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 and the PSMB.

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 liable for the settlement risks associated with the sponsored payment institution.

8.1.11 A sponsored payment institution must submit a 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 the PSMB, and confirming that it will settle the payment obligations on behalf of the sponsored payment institution.

Part 3: Application to conduct a payment activity

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 more than R5 million average monthly transaction values must issue e-money in an interoperable payment system and apply to the Reserve Bank for authorisation as a Tier 1 e-money issuer.

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 18 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 client funds received for e-money;

9.4.3 issue e-money at face value on the receipt of funds;

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 bank account/trust 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 ensure that the onboarding processes in respect of clients are risk-proportionate and comply with applicable anti-money laundering, combating the financing of terrorism and counter proliferation financing (AML/CFT/CPF) legislation;

9.4.8 ensure that the Tier 1 e-money issuer and their agents comply with the applicable provisions of the AML/CFT/CPF legislation and the regulations/directives issued in terms of such legislation;

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

a. per individual – for natural persons: R15 000.00 per day and R50 000.00 per month or as may be amended by the Reserve Bank from time to time; and

b. for juristic persons: R100 000.00 per month per entity or as may be amended by the Reserve Bank from time to time;

9.4.10 must not have a maximum outstanding e-money balance on e-money accounts which exceeds:

a. natural person: R100 000.00 or as may be amended by the Reserve Bank from time to time; and

b. juristic person: R500 000.00 or as may be amended by the Reserve Bank from time to time; and

9.4.11 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 9.4.9 and 9.4.10 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 by the Reserve Bank and the PSMB or appoint a clearing system participant, 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 and participate in the relevant PCHs/scheme or appoint an authorised PSMB member to participate in the relevant PCH/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, if settlement is in the Reserve Bank settlement system subject to the sponsorship or direct access requirements under paragraph 8, or be designated as a settlement system participant or appoint a designated settlement system participant to settle payment obligations on its behalf subject to the sponsorship requirements under paragraph 8; and

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, the PCH system operators and operators of settlement systems and designated settlement systems, as the case may be.

9.7 Where a Tier 1 e-money issuer holds payment accounts or issues payment instruments, it must conduct client/customer due diligence in accordance with the FIC Act.

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 15 of Annexure A;

10.1.3 where a Tier 1 e-money issuer appoints an agent or enters into outsourcing arrangements, comply with paragraphs 16 and 17 of Annexure A and provide information to the Reserve Bank as per Annexure F;

10.1.4 commence actual engagement in 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 (Failure to commence actual e-money issuance within the 12-month period or longer period as approved by the Reserve Bank will render the authorisation automatically revoked.); and

10.1.5 notify the Reserve Bank of any amendments to the information provided in their initial application. (Such notification must be submitted within thirty (30) calendar 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 transaction values below R5 million in the interoperable payment system must apply to the Reserve Bank for authorisation as a Tier 2 e-money issuer.

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 18 of Annexure A.

11.4 A Tier 2 e-money issuer is exempted from complying with paragraphs 2.2.2, 7.4 and 7.5.1 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 be a juristic person incorporated in the RSA as set out in paragraph 2 of Annexure A;

11.5.2 must not issue e-money accounts with an individual transaction limit that exceeds R5 000.00 per day and R20 000.00 per month or as may be amended by the Reserve Bank from time to time, per natural or juristic persons;

11.5.3 must not have a maximum outstanding e-money balance on e-money account which exceeds R20 000.00 per natural or R50 000.00 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 a 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 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;

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 and participate in the relevant PCHs/scheme or appoint an authorised PSMB member to participate in the relevant PCH/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;

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 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, the PCH system operators and operators of settlement systems, as the case may be;

11.6.5 ensure that the Tier 2 e-money issuer and their agents comply with the applicable provisions of the AML/CFT/CPF legislation and the regulations/directives issued in terms of such legislation; and

11.6.6 conduct simplified AML/CFT/CPF customer due diligence on its clients.

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

12.1.2 comply with the requirements under paragraphs 5 to 15 of Annexure A;

12.1.3 ensure that the onboarding processes in respect of clients are risk-proportionate and comply with applicable AML/CFT/CPF legislation and the regulations/directives issued in terms of such legislation;

12.1.4 conduct simplified AML/CFT/CPF customer due diligence on its clients;

12.1.5 where a Tier 2 e-money issuer appoints an agent or enters outsourcing arrangements, comply with paragraphs 16 and 17 of Annexure A, and provide information to the Reserve Bank as per Annexure F; and

12.1.6 inform and notify the Reserve Bank of any changes to the information submitted in the original application within thirty (30) business days of such a 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, 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;

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

c. where redemption is requested more than one year after the date of termination of the contract; any such fee must be proportionate and commensurate with the actual costs incurred by the e-money issuer.

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. Application 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 information prescribed therein.

14.3 A person that seeks authorisation to issue payment instrument must meet the general requirements in paragraphs 2 to 4 and 6 to 8 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 relevant scheme(s) and ensure full compliance with all 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; and

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

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

15.1.2 comply with paragraphs 5, 10, 11, 13, 14 and 15 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;

15.1.5 ensure that appropriate means are at all times available to enable the client 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 of any changes to the information submitted in the original application within thirty (30) business days of such change.

Group B: Acquiring

16. Authorisation requirements for acquiring a payment activity

16.1 A person who seeks to conduct an 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 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 a minimum capital and comply with the prudential requirements as set out in the Annexure D;

16.4.2 become a member of relevant authorised scheme(s);

16.4.3 participate in relevant PCH arrangement(s);

16.4.4 be a clearing system participant or appoint a Reserve Bank settlement system participant to clear payment instructions and settle payment obligations on its behalf in accordance with section 4(2)(d) of the NPS Act; and

16.4.5 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.

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 such as information on business ownership and/or management;

b. business office and/or store address, 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;

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 at all times, 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, 12, 13, 14 and 15 of Annexure A;

17.1.4 verify and record the true identity of their payees and representatives;

17.1.5 conduct customer/payee due diligence;

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

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

17.1.8 keep records of these monitoring activities;

17.1.9 ensure transparency of charges/fees to payees;

17.1.10 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.);

17.1.11 ensure timely and complete /payments with payees within the payment period agreed upon by the acquirer and the payee, which shall not be longer than two (2) business days from the day the funds are received by the acquirer for transfer to a payee (If the payment cycle stated in the user agreement is more than the agreed maximum number of days as stated above, an acquirer must submit justification, including supporting documentation, to the Reserve Bank, and such extended payment cycle shall be subject to prior approval of the Reserve Bank. The acquirer must safeguard the outstanding payee funds as set out in paragraph 9 of Annexure A.);

17.1.12 provide the collected funds to payees in the event the issuer of payment instruments or any other parties involved in the handling of such funds fail to fulfil their settlement obligations, regardless of disputes with other parties;

17.1.13 commence actual engagement in acquiring 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 acquiring within the 12-month period shall render the authorisation automatically revoked.); and

17.1.14 inform and notify the Reserve Bank 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 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 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 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 authorised or DCSP;

18.5.7 specify the PCHs or schemes the person seeking designation or authorisation to clear seeks to participate in;

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

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

18.5.10 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 20.2 below; and

18.5.11 specify whether it will clear payment instructions on behalf of other payment institutions.

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 at all times, 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 of any changes to the information submitted in the original application within thirty (30) business days of such change.

20. Settlement

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

20.1 A person who seeks to participate in a cross-border designated settlement system is exempted from applying to the Reserve Bank for authorisation to participate in the cross-border designated settlement system. The person must comply with the application requirements set out by the operator of the cross-border designated settlement.

20.2 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.

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

20.4 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.

20.5 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:

20.5.1 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;

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;

20.5.2 where a person seeks to participate in the designated settlement system, such person may be the Reserve Bank, a bank or non-bank payment institution that is a DCSP;

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

20.5.4 obtain membership in the relevant scheme(s) and participation in the relevant PCHs;

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

20.5.6 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 at all times, 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, 11, 13, 14 and 15 of Annexure A;

21.1.3 comply with paragraph 16 of Annexure A if it intends to appoint an agent; and

21.1.4 comply with paragraph 17 of Annexure A if it intends to enter into outsourcing arrangements.

22. Application to operate a settlement system

22.1 A person other than the Reserve Bank who seeks to operate a designated settlement system must apply to the Reserve Bank for designation in accordance with section 4A of the NPS Act to operate such a settlement system.

22.2 An application under paragraph 22.1 must meet the requirements as set out in section 4A of the NPS Act. This Directive is not applicable to a designated settlement system.

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

22.4 Notwithstanding the exemption from authorisation, the Reserve Bank as the Reserve Bank settlement system operator must meet the general requirements in paragraphs 7, 8, 13 and 15 of Annexure A.

22.5 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 its settlement system and dispute resolution rules;

c. admit settlement system participants that comply with the criteria referred to in paragraph 22.5a;

d. enforce participation rules on its settlement system participants; and

e. with the prior approval of the Reserve Bank, terminate admission of a participant in the settlement system.

22.6 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.

22.7 The Reserve Bank may issue an instruction to a settlement system operator, directing it to amend the rules in a particular manner to address issues identified by the Reserve Bank.

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

22.8.1 maintaining settlement accounts;

22.8.2 settlement finality;

22.8.3 risk mitigation;

22.8.4 liquidity provision;

22.8.5 operating procedures and times;

22.8.6 data protection and security; and

22.8.7 recovery of the settlement system.

22.9 A Reserve Bank settlement system operator must:

22.9.1 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;

22.9.2 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;

22.9.3 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;

22.9.4 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

22.9.5 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 initiating payment instructions.

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 information prescribed therein.

23.2.3 A person who seeks to provide a payment initiation activity must meet the general requirements in the paragraphs 2 to 4, 6, 7 and 8 of Annexure A.

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

23.3.1 at the time of authorisation, hold a 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 referred to in paragraph 23.8.2(d);

23.3.4 not hold a payer's funds in connection with the provision of payment initiation activity at any time; and

23.3.5 on an ongoing basis, inform and notify the Reserve Bank 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. transmit the payer's security credentials through safe and efficient channels, including encryption methods, and not transmit the payer's security credentials to any other party except the payer;

c. 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;

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

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

f. 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 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 prioritise the processing of payment instructions.

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 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 widely recognised industry standards;

c. comply with all requirements, where applicable, as provided for in the personal data 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 recognised 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 and other sensitive payment data 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-permissioned data which complies with the POPI Act (The process to collect this data must be simple, standardised and secure, and include the reason given for the purpose the data is collected.);

b. issue/initiate a payment instruction only when the payer has given informed consent for the issuing of the payment instruction (The payer must authorise a payment instruction before a payment initiation service provider initiates the payment instruction, unless the payer and the payment initiation service provider have agreed on the authorisation after the issuing/initiation of a payment instruction.); and

c. 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 must be able to 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.

23.7 Authentication

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

a. accesses the payment account online;

b. initiates an electronic payment transaction; and

c. 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:

a. apply strong client authentication for every transaction; and

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

23.7.3 A payment initiation service provider must apply strong client authentication when the payer instructs it to initiate a payment instruction.

23.8 Obligations for interface infrastructure

23.8.1 In respect of their interface with each other, a payment account service provider and a payment initiation service provider must:

a. develop and implement an interface infrastructure that enables:

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

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

23.8.2 The interface infrastructure must:

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

b. enable a 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;

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

e. 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 Contingency measures for interface infrastructure

23.9.1 The payment account service provider and payment initiation service provider must:

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

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

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

23.9.2 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.

23.9.3 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 For payment initiation, the payment account service provider must:

a. refund the payer, within 48 hours, the amount of unauthorised or incorrectly facilitated transactions 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, prove 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 it believes that the payer acted fraudulently or with intent or gross negligence, provide supporting evidence to prove fraud, intent or gross negligence on the part of the payer.

23.10.3 The payment initiation service provider must:

a. where a payer denies having authorised a payment instruction, prove 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 it believes that the payer acted fraudulently or with intent or gross negligence, provide supporting evidence to prove fraud, intent or gross negligence on the part of the payer; and

c. within 48 hours, compensate the payer for the losses incurred or refund the payer should it be liable for an unauthorised payment transaction.

23.10.4 The payment account service provider must:

a. ensure that the payer utilises 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 user/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. ensure that the payment account service user/payer does not bear any financial losses where the payment account service provider does not require 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. bear 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 23.10.3 and 23.10.4 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 and the nature of the transaction.

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

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 more than R5 million average monthly transaction values 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 equal to or less than R5 million average monthly transaction values 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 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.

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 **Segregated bank account:** open and maintain a segregated bank account and safeguard the client funds, and provide evidence of such an account at application.

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

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

27.1.2 aggregated annual volumes and values per payment activity processed;

27.1.3 aggregated annual amounts deposited in payment accounts for the various payment activities; and

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

28. Fit-and-proper requirements

28.1 A payment institution 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 The 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 data; 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/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, provide their names and physical addresses.

31. Agency arrangements

31.1 A TPPP may use an agent/s to conduct a TPPP payment activity, subject to paragraph 16 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 17 of Annexure A.

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

33.1 A person that provides payments to third persons/parties must, on an ongoing basis:

33.1.1 at all times, 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, 10, 11 and 14 of Annexure A;

33.1.4 conduct due diligence when onboarding clients;

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

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

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

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

c. obtain a certified copy of the proof of physical 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 12 of Annexure A, such interest shall accrue to the TPPP and shall not be paid to the client.

33.3 The TPPP:

33.3.1 must make payment to a beneficiary in accordance with the frequency and timeline as agreed between the TPPP and its clients, provided that beneficiary funds are not held for more than 30 days after receipt of payments from the payer/s;

33.3.2 may use an agent for agency business in accordance with agency arrangements requirements set out in paragraph 16 of Annexure A and F; and

33.3.3 may enter into outsourcing arrangements in compliance with paragraph 17 of Annexure A.

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 transaction with 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, and must retain such records for five (5) years from the record date.

34.2 When receiving funds from a payer to distribute as a single transaction to multiple beneficiaries, the TPPP must record each transaction with 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, and must retain such records for five (5) years from the transaction date.

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 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 processing or clearing business/activities and avoid bundling scheme and processing or clearing fees;

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 operating a scheme; and

35.4.7 disclose its fees to its members and avoid bundling of scheme and 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 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 admission of a member in a scheme.

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

36.3 Where the Reserve Bank issues an instruction to a 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 11 of Annexure A.

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 of 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 operate on an ongoing basis and limit

losses in the event of a 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 implementation of:

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 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 more than R5 million average monthly transaction values 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 information prescribed therein.

38.3 A Tier 1 money remitter must meet the requirements in paragraphs 2 to 4, 6 to 8 and 18 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;

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; and

38.4.3 must notify the Reserve Bank immediately after opening a money remittance outlet.

38.5 A Tier 1 money remitter that provides 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 R5 000 per day per client with a limit of R50 000 per client per calendar month.

38.6 Where 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 following the 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.

38.7 The Tier 1 money remittance must:

38.7.1 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;

38.7.2 where the Tier 1 money remitter is either a bank or a non-bank, 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;

38.7.3 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; and

38.7.4 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.

39. Ongoing requirements for Tier 1 money remitters

39.1 On an ongoing basis, a Tier 1 money remitter must:

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

39.1.2 comply with the requirements in paragraphs 5 to 15 of Annexure A;

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

39.1.4 where the Tier 1 money remitter appoints an agent or enters into outsourcing arrangements, comply with paragraphs 16 and 17 of Annexure A and F; and

39.1.5 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 A Tier 1 money remitter must conduct due diligence on its clients.

39.4 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.

39.5 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.

39.6 A money remitter must transfer to the payee all funds in real time, immediately upon receipt.

39.7 Where 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 following the day of receipt of the funds, such funds must be kept in a segregated account/trust account and safeguarded as set out in paragraph 9 of Annexure A. The Tier 1 money remitter must provide evidence of such an account at application.

39.8 A money remitter must at all times demonstrate that it can reconcile the funds paid into its clients' trust account (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 conducts interoperable money remittances on a limited scale equal to or below R5 million average monthly transaction values shall 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 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 18 of Annexure A.

40.4 A Tier 2 money remitter is exempted from complying with paragraphs 7.2 and 7.3 of Annexure A.

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

40.5.1 at the time of authorisation, such a person holds minimum capital and complies with the prudential requirements as set out in Annexure D; and

40.5.2 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.

40.6 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.

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

40.7.1 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;

40.7.2 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; and

40.8 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.

41. Ongoing requirements for Tier 2 money remitters

41.1 The money remitter must, on an ongoing basis:

41.1.1 not conduct money remittance with an individual transaction limit that exceeds R2 500 per day and a limit of R25 000 per payer per calendar month or as may be amended by the Reserve Bank from time to time;

41.1.2 at all times maintain ongoing capital and comply with the prudential requirements as set out in Annexure D;

41.1.3 notify the Reserve Bank prior to opening an outlet or branch;

41.1.4 where a money remitter has more than one account with a bank, 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, immediately upon receipt;

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

41.1.8 comply with the requirements under paragraphs 7 to 15 of Annexure A;

41.1.9 comply with paragraph 16 of Annexure A as well as Annexure F if it intends to enter into agency business;

41.1.10 comply with paragraph 17 of Annexure A if it intends to enter into outsourcing arrangements;

41.1.11 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

41.1.12 conduct simplified and risk-based due diligence on its clients.

Part 4: Closed-loop payment system or payment activity

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 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 closed-loop payment system operator 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, parking ticketing, 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 falls 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 the closed-loop payment system will be operational;

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

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

42.5.16 audited financial statements for the past three (3) years or, if the applicant is newly established, projected financial statements for the next three (3) years, including income statements, balance sheets and cash flow statements;

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 18 of Annexure A.

42.6 Where a closed-loop payment system holds payment accounts or executes low-value transactions of under R10 000, it must conduct simplified customer due diligence on its clients.

42.7 Where a closed-loop payment system holds payment accounts, issues payment instruments or executes low-value transactions of over R10 000, it must conduct customer due diligence.

42.8 The total value of payment transactions executed in the closed-loop payment system over the preceding 12 months or forecast over 12 months must not exceed the amount of R3 million.

42.9 Where the transactions exceed R3 million, the operator or provider of the closed-loop payment system payment activities must notify the Reserve Bank to assess whether or not the closed-loop system operator must apply for authorisation as a payment institution to operate or provide the payment activity in the interoperable environment.

42.10 The closed-loop payment system provider should calculate the threshold at the level of each issuer. Where a single operator/issuer conducts payment activities based on more than one specific payment instrument, the calculation of the threshold should be carried out by combining all the payment transactions executed with all specific payment instruments offered by the same issuer.

42.11 Persons that operate a closed-loop payment system or conduct payment activities within the closed-loop system must apply for authorisation within ninety (90) 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, 11, 13 and 14 of Annexure A.

43.2 The payee's payment 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 service provider's account.

43.3 Inform and notify the Reserve Bank of any changes to the information submitted in the original application within thirty (30) business days of such 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, 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 an agent, master agent or payment institution;

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

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

44.4.4 direct a payment institution to terminate the agency agreement; 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 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 other prescribed requirements which the Reserve Bank may issue.

44.6 The list of agents will be published on a monthly basis on the Reserve Bank's website.

44.7 The Reserve Bank will exercise its discretion to determine which scheme rules will apply. If there is a conflict of rules between different schemes, the Reserve Bank will decide which scheme rules take precedence.

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 a 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 the Reserve Bank representatives reasonably require;

45.6.6 if not practicable or appropriate to meet a requirement in terms of subparagraph 48.6.5, 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 ensure that the Reserve Bank can effectively regulate, supervise and oversee their activities, systems, data and operations related to authorised, designated and registered payment activities.

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

46.1 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:

46.1.1 varying a condition of a participation mechanism;

46.1.2 adding a condition;

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

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

46.2 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:

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

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

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

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

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

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

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

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

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

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

46.5 The period referred to in paragraph 46.4.2 must be at least one (1) month.

46.6 The Reserve Bank need not comply with paragraph 46.4.1 and 46.4.2 if the payment institution has applied for the variation, revocation or suspension.

46.7 The Reserve Bank shall publish, on its website, the notices relating to the variation, suspension or revocation of authorisation and exemption.

47. Conclusion

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

47.2 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.

47.3 This Directive will become effective within three (3) months from the date of publication. For the entities that are already authorised, designated and/or registered, the transitional arrangements specified in Annexure E shall be applicable.

47.4 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

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

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 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 shareholder 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 The payment institution must establish and maintain effective policies, procedures and controls to ensure timeous reporting of unusual and/or suspicious transactions by staff. These measures must include the maintenance and provision of all relevant records and data to the designated AML/CFT Compliance Officer for further analysis and determination of whether the transaction should be reported to the FIC. 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:

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.

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.
d. The person has accepted civil liability or is civilly liable for theft, fraud, forgery, uttering a forged document, misrepresentation or dishonesty under any law.
e. The person has seriously or persistently failed to, or is failing to, manage any of his/her financial obligation (including debts) satisfactorily, including the person has been subjected to sequestration proceedings.

f. 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.

g. 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.

h. 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.

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

j. The person has breached fiduciary duties.

k. 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.

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

m. 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.

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

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

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

q. 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, notifying the Reserve Bank of such an assessment and outcome as well as ensuring 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;

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;

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

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

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

7.7 For payment initiation, a payment initiation service provider must perform due diligence on their clients prior to entering into contractual arrangements and on an ongoing basis.

7.8 Due diligence must include at least the following:

7.8.1 verification of the true identity of the client;

7.8.2 establishment of whether the client's business is legal and/or registered with the relevant authorities;

7.8.3 understanding the business activity of a client;

7.8.4 regular monitoring of a client's transactions for any irregularities; and

7.8.5 keeping information obtained for the purpose of establishing and verifying the identities of clients in line with the record-keeping requirements.

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 at least an annual formal review of the information data security risk assessment for the enterprise security arrangements, with ongoing action plans, supported by detailed information security assessments on high-risk areas performed 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, 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 for cyber protection 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 bank account maintained at a bank;

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 bank 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.

9.3 A payment institution may additionally cover client funds through an insurance policy or another comparable guarantee. This policy must be issued by an insurance company that is not part of the same group as the payment institution. 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 may be required to transfer a portion of the funds from the account where such client funds are 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.

10. Anti-money laundering, counter terrorism financing and counter proliferation financing (AML/CTF/CPF)

10.1 Unless exempted by the Reserve Bank, payment institutions (including payment institutions that are not accountable institutions) must:

10.1.1 comply with chapter 3 of the FIC Act and supporting guidance/public compliance communication on AML/CFT/CPF and related activities and financial sanctions control measures, especially the following sections:

a. Part 1: customer due diligence;
b. Part 2: duty to keep record;
c. Part 2A: financial sanctions;
d. Part 3: reporting duties and access to information;
e. Part 4: measures to promote compliance; and
f. Part 5: referral and supervision;

10.1.2 comply with chapter 4 of the FIC Act and supporting guidance on compliance and enforcement;

10.1.3 comply with chapter 5 of the FIC Act and supporting guidance on miscellaneous;

10.1.4 comply with AML/CFT/CPF regulations; and

10.1.5 comply with POCDATARA.

10.2 The Reserve Bank may require the submission of AML/CFT/CPF risk controls at any time, and may conduct on-site or off-site inspections to assess compliance.

10.3 Failure to maintain adequate AML/CFT/CPF measures or to comply with any requirement in this section constitutes grounds for licence suspension.

10.4 The Reserve Bank, as a supervisory body in terms of the FIC Act, must implement risk-based approach supervision on the above requirements for proportionality and financial inclusion.

11. Accounting and audit

11.1 A payment institution must:

11.1.1 maintain accounting records on a continual basis and prepare financial statements that conform with the International Financial Reporting Standards and any other generally accepted accounting practices;

11.1.2 have these records and annual financial statements audited by external auditors;

11.1.3 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

11.1.4 submit the information and identities of external auditors or firms, along with their names, addresses, the frequency of the audits and contact details.

11.2 Internal audit function

11.2.1 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.

11.2.2 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.

11.2.3 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.

12. Interest earned

12.1 Client funds held in a segregated bank account or settlement account in a designated settlement system 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 bank account.

12.2 The payment institution must offer low-fee products and services as a result of interest earned.

12.3 The clients of the payment institution shall not earn interest on the client funds held in the segregated bank account.

13. Value date and availability of funds

13.1 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:

13.1.1 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

13.1.2 in the absence of the timelines as set out in 13.1.1, 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 payment institution.

13.2 A payment institution shall ensure that payments or transactions from a payer's payment account are made in accordance with the payer's consent.

14. Prohibitions and restrictions

14.1 A payment institution, other than a bank and the payment institution providing payment account type B of Group G, must not use client funds for any credit/lending or investment activities.

14.2 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.

15. Disclosure of charges

15.1 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. These clients are a specific group of users that the payment institution intends to serve with its products and services.

16. Agency arrangements

16.1 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 16.2.

16.2 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.

16.3 The payment institution is accountable for the actions and omissions of its agents when those actions fall within the scope of the agency agreement.

16.4 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.

16.5 An authorised payment institution providing third-party payments may appoint any person or another authorised payment institution providing third-party

payments as a pay-in or pay-out agent, under governance of an agent agreement that must be compliant with the agency agreement requirements.

16.6 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.

17. Outsourcing arrangements

17.1 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 to an entity forming part of the same group as the payment institution.

17.2 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.

17.3 An operational function is considered important if a defect or failure in its performance materially impairs:

17.3.1 the payment institution's continual compliance with this Directive; or

17.3.2 the financial performance, soundness or continuity of the payment institution's activities.

17.4 An outsourcing arrangement under this paragraph must comply with the following conditions:

17.4.1 the senior management of the payment institution must retain accountability and must not delegate it;

17.4.2 the relationship and obligations of the payment institution towards its clients shall not be altered;

17.4.3 the outsourcing shall not amend, suspend or revoke a condition of the payment institution; and

17.4.4 any other conditions that the Reserve Bank may specify.

17.5 A payment institution must:

17.5.1 establish a service level agreement for all outsourcing arrangements; and

17.5.2 submit copies of it to the Reserve Bank within ten (10) business days of its signing.

17.6 A payment institution that engages in outsourcing arrangements must provide to the Reserve Bank:

17.6.1 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;

17.6.2 the identity of the persons that are responsible for each of the outsourced activities;

17.6.3 a clear description of the outsourced activities and their main characteristics;

17.6.4 confirmation that the outsourcing service provider has business continuity and disaster recovery plans in place that are regularly tested;

17.6.5 a copy of the draft outsourcing agreements; and

17.6.6 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.

18. Client complaints

18.1 A payment institution must provide:

18.1.1 a description of the structure and process for handling client complaints, including escalation procedures and service channels; and

18.1.2 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: Acquirers a. Acquirer	 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 000.00
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 000.00

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 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. 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 the level 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 biannually provide the Reserve Bank with audited financial statements for the preceding six-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. A 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 a 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. cash 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

	Payment activity	**Transitional arrangements**
Group A1: E-money		
	Issuing of e-money (linked to Payment Account C)	**New:** All e-money issuers, whether a bank or non-bank, apply from the publication date of the Directive. **Current:** E-money issuers (including mobile money providers) operating in closed loop systems (banks and non-banks), apply from the publication date of the Directive.
Group B: Acquiring		
	Acquiring of payment instructions	**New:** Must apply from the publication date of the Directive. **Current:** Banks and non-banks from the publication 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 publication date of the Directive. **Current:** Clearing or settlement system participants – within three (3) months from the publication date to apply.
	Payment initiation	**New:** Apply from the publication date of the Directive. **Current:** Continue with the registration requirements under Directive 2 of 2024 and apply from the publication date of the Directive.
Group E: TPPP/payments to third persons		
		New: Apply six (6) months after the publication of the Directive. **Current:** Continue with the mandatory sponsorship and within six (6) months after the publication operate under the current regime and reapply six (6) months after the publication of the Directive.
Group F: Schemes		
	Schemes	**Current and new:** New schemes (i.e. schemes established after the publication 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 date of the publication 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 publication of the Directive. **Current:** Existing money remitters that have partnered with banks or are authorised dealers with limited authority... (ADLAs) apply four (4) months after the publication of the Directive.

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 name and address of the agent;

b. where applicable, the unique identification code or number of the agent;

c. 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;

d. 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;

e. agency services to be provided through the agent;

f. the proposed geographical coverage of the agent over a three-year period;

g. the due diligence policy and procedures conducted on the agent and the payment institution's due diligence report on the agent;

h. the IT systems, processes and infrastructure that are used by the agents to perform activities on behalf of the payment institution;

i. the selection policy, monitoring procedures and agents' training;

j. copies of all draft agency agreements;

k. 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;

l. an internal audit report regarding internal controls to be used for agency business and for any master agent;

m. the AML/CFT/CPF policies and procedures as they relate to agency business, including Know Your Customer (KYC) procedures, if applicable;

n. 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;

o. a policy document on how the payment institution will address the risk of the agent overselling or overcharging; and

p. 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. 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;

m. 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

n. 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 to operate 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: R25 000 Per month: R100 000 **Juristic persons:** Per month: R500 000	**Natural persons:** R100 000 **Juristic persons:** R500 000
	Tier 2 (small scale): < R5 million average monthly transaction values	**Natural and juristic persons:** Per day: R5 000 Per month: R50 000	**Natural and 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