SOUTH AFRICAN RESERVE BANK

NO. 5550 **15 November 2024**

SOUTH AFRICAN RESERVE BANK

Directive in respect of issuing of electronic funds transfer credit payment instructions on behalf of the payer in the national payment system

Directive No. 2 of 2024

Contents

1. **Definitions** 2
2. **Background** 5
3. **Purpose** 8
4. **Scope of this directive** 8
5. **Directive** 8
6. **Supervision and compliance monitoring** 17
7. **Effective date and non-compliance** 22
8. **Conclusion** 22

1. Definitions

1.1 Unless the context indicates otherwise where the interpretation should further be in the context of this directive, any word or expression used in this directive to which a meaning has been assigned in the National Payment System Act 78 of 1998, as amended (NPS Act), has that meaning.

1.2 **Beneficiary** refers to a person that is identified by the payer as the receiver of the funds associated with the electronic funds transfer credit.

1.3 **Clearing system participant** is a person defined as such in section 1 of the NPS Act.

1.4 **Critical staff** means a natural person that performs functions that are essential to the operations of a person issuing electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping, including a person who has access to information technology (IT) systems.

1.5 **Cyberattack** means malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt or gain unauthorised access to IT systems.

1.6 **Cyber-event** means any observable occurrence in an information system. Cyber-events sometimes provide an indication that a cyber-incident is actually occurring.

1.7 **Cyber-incident** means a cyber-event that adversely affects the cybersecurity of an information system and/or the information that the system processes, stores or transmits, or which violates the security policies, security procedures and/or acceptable use policies, whether resulting from malicious activity or not.

1.8 **Data breach** means a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.

1.9 **Due diligence** means the identification, understanding and obtaining of information about the business relationship of a beneficiary of the payment.

1.10 **Electronic funds transfer credit** means a payment instruction carried out by electronic means on behalf of a payer, with a view to making an amount of funds available to a beneficiary, irrespective of whether the payer and the beneficiary are the same person.

1.11 **Electronic wallet** is a digital representation of value that is stored electronically on an electronic device.

1.12 **FIC Act** means the Financial Intelligence Centre Act 38 of 2001, as amended.

1.13 **Faster payments** refer to a low-value, credit-push payment service in which both the transmission of the payment message and the availability of funds to the beneficiary occur in real time or near-real time, on a basis that the service is available 24 hours a day, 7 days a week (24/7).

1.14 **Fraud** refers to the issuing of a payment instruction with the intention to defraud a person.

1.15 **Front-end interface** is the point at which a payer interacts with a website or application.

1.16 **Governing body** refers to a person or body of persons, whether elected or not, that manages, controls and formulates the policy and strategy of the person issuing electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping; directs its affairs; or has the authority to exercise the powers and perform the functions of the person issuing

electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping.

1.17 **Informed consent** means any voluntary, specific and informed expression of will in terms of which permission is given by the payer for the processing of the payer's online banking credentials.

1.18 **Payer** is a person that holds a payment account and allows a payment instruction to be issued from that payment account.

1.19 **Payment instruction** is an instruction to transfer funds or make a payment, as defined in section 1 of the NPS Act.

1.20 **Person** refers to a natural or juristic person and includes a trust.

1.21 **POPI Act** means the Protection of Personal Information Act 4 of 2013.

1.22 **Scheduled payment transaction** is a payment that is scheduled by the payer for a specific date as agreed between the payer and the beneficiary.

1.23 **Screen scraping** in payments means the use of computer techniques to solicit the payer's online banking login credentials to access the clearing system participant's online banking website to issue an electronic funds transfer credit payment instruction on behalf of the payer.

1.24 **Sort-at-source** means the practice of sorting payment instructions based on multiple holders of destination accounts and submitting such payment instructions directly to the holders of the destination accounts or requesting clients to pay directly into specific accounts (e.g. third-party payment providers' or beneficiaries' accounts), resulting in the bypassing of the clearing system, which is undertaken through regulated acquiring or sponsoring relationships.

2. Background

2.1 In terms of section 10(1)(c) of the South African Reserve Bank Act 90 of 1989, as amended (SARB Act), the South African Reserve Bank (SARB) 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 NPS Act provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in the Republic of South Africa and for connected matters.

2.2 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, assisting transacting parties to make payments and exchange value.

2.3 The SARB is empowered in terms of section 12 of the NPS Act to issue directives, after consultation with the payment system management body, to any person regarding a payment system or the application of the provisions of the NPS Act. Currently, the Payments Association of South Africa is recognised by the SARB in section 3 of the NPS Act as a payment system management body to organise, regulate and manage the participation of its members in the payment system.

2.4 In recent years, the payment industry has witnessed the emergence of financial technology (fintech) companies that leverage technology to offer innovative tools, products and services. These tools, products and services are offered particularly in the e-commerce environment with minimal regulatory oversight. One such tool is screen scraping, which is used by a person, usually a fintech company, in partnership with beneficiaries, to conduct screen scraping to issue electronic funds transfer credit payment

instructions. Although screen scraping is popular in e-commerce payment transactions, it is now growing in usage in other payment activities such as bill payments and the funding of electronic wallets, which are facilitated by a person that issues electronic funds transfer credit payment instructions on behalf of payers.

2.5 Screen scraping is largely conducted without the informed consent of the payer, the understanding of the implications of sharing the credentials as well as using the branding of clearing system participants without approval. This practice exposes the NPS, including the participants and payers to risks such as those stipulated in paragraphs 2.5.1 to 2.5.6. These risks have a negative impact on the integrity, efficiency, security and confidence in the NPS. These risks include but are not limited to:

2.5.1 Lack of informed consent and understanding of the implications of sharing the credentials: Many payers that use the front-end interface of a person issuing electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping, are not informed that by entering their online banking credentials, they are not logging on to their actual clearing system participant's proprietary online banking platform and do not understand the implications of sharing their credentials. Instead, they are sharing their online banking credentials with a person to issue electronic funds transfer credit payment instructions on their behalf. The use of payers' online banking credentials without their informed consent and understanding of the implications in so doing has a negative impact on the integrity of payments and security of the NPS.

2.5.2 Misleading perception that the payment is instant: A person issuing electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping, usually markets its service as providing an 'instant or fast payment' to the beneficiary's account. This is misleading as a normal electronic funds transfer credit payment instruction does not necessarily result in the funds being credited into the beneficiary's account instantly unless the payer chooses the faster payments option to process the payment

into the beneficiary's transactional account, or a transaction is an intrabank (on-us) transaction processed directly into the beneficiary's transactional account. Misleading payers and beneficiaries that the payment is instant undermines the integrity of payments and confidence in the NPS.

2.5.3 Conducting sort-at-source: A person may use screen scraping to perpetuate the sort-at-source practice by using bank accounts from multiple banks to ensure that payments are on-us transactions, resulting in an 'instant' payment. Conducting sort-at-source negatively impacts the NPS as it goes against the SARB's objectives of promoting efficiency, safety, interoperability, transparency, modernisation and optimisation of interchange fees.

2.5.4 Lack of data privacy: Screen scraping puts payers' online banking credentials at risk of being compromised. Payers have no control over how their credentials and any other data or personal information are accessed, processed, used and stored by the person issuing an electronic funds transfer credit payment instruction on their behalf (e.g. account numbers and account statements may be stored and utilised without the payer's informed consent). This undermines the public's trust and confidence and security of the NPS.

2.5.5 Exposure to fraud: Rogue entities may pose as persons issuing electronic funds transfer credit payment instructions on behalf of payers, using screen scraping, on fraudulent e-commerce sites to capture payers' online banking access credentials. Such entities may impersonate the payer and conduct any activity that the payer would have access to on their online banking platform (e.g. making real-time payments to themselves, applying for a personal loan, increasing transaction limits and ultimately initiating payments to mule transactional accounts). Similar to a lack of data privacy, fraud weakens the public's trust, and confidence in and integrity and security of the NPS.

2.5.6 Risk of financial loss or non-delivery of the goods/services purchased: electronic funds transfer credit payments are final and irrevocable in nature and payers may face challenges when lodging disputes to reverse a transaction in the event of the beneficiary not honouring the agreement (e.g. not delivering the goods or delivering incorrect or counterfeit goods). Payers might also be held liable for the interest payable on such amounts when payment was made from the credit card account or overdraft facilities of the payer. This would significantly and negatively impact the efficiency, integrity and security of the NPS.

3. Purpose

3.1 The purpose of this directive is to impose requirements on persons issuing electronic funds transfer credit payment instructions on behalf of the payer, using screen scraping, or any other tool in the NPS to mitigate the risks identified in paragraph 2.5.

4. Scope of this directive

4.1 This directive applies to any person issuing payment instructions on behalf of a payer, using screen scraping, or a similar tool in the NPS.

5. Directive

5.1 Registration requirements

5.1.1 No person may issue electronic funds transfer credit payment instructions on behalf of a payer in the NPS unless that person:

a. is registered with the SARB in the manner and form prescribed by the SARB; and
b. has obtained informed consent of the payer prior to issuing such a payment instruction or initiating such a payment; or
c. has been exempted from registration by the SARB.

5.1.2 A juristic person must apply for registration with the SARB to issue payment instructions or initiate payment on behalf of a payer.

5.1.3 The application to register with the SARB must be addressed to the Head of the National Payment System Department at npsdirectives@resbank.co.za.

5.1.4 The application for registration must be accompanied by the following information and supporting documents:

a. proof of business registration and/or founding documents of a juristic or legal person, issued by the applicable competent South African authorities;
b. proof of physical address of the place of business in South Africa;
c. disclosure of ownership, including the names and certified copies of the identity documents of the shareholders, trustees and ultimate beneficial owners;
d. organisational structure;
e. the types and sources of funding, including the capital contribution for the establishment and operation of the business. In the case of a loan, the funding details of the name of the lender and their domicile must also be provided;
f. a reasonably measurable forecast budget calculation for the next three financial years which demonstrates that the applicant is able to employ appropriate systems, resources and procedures to operate in a sound manner; and
g. a description of the applicant's governance arrangements and internal control mechanisms relating to, inter alia, IT systems, data security, administrative, risk management and accounting procedures, which demonstrates that these governance arrangements, control mechanisms and procedures are appropriate, sound and adequate.

5.2 Conditions for registration

5.2.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. employ or appoint a qualified person(s) with relevant experience responsible to ensure compliance with the relevant legislation, rules, regulatory frameworks and agreements;
b. employ or appoint a qualified person(s) with relevant experience responsible for risk management, including but not limited to fraud risk, operational risk and IT risk, and compliance function;
c. be satisfied that the key person(s) is honest and has integrity;
d. furnish the SARB with the curriculum vitae and copies of supporting documents, including but not limited to the identity document, proof of physical address and certificates of qualifications of a key person(s) upon their appointment;
e. demonstrate to the SARB, subject to the approval of the SARB, the manner in which informed consent will be requested from payers;
f. where it is not acting as a beneficiary, have clear and transparent policies and procedures approved by its governing body for on-boarding beneficiaries;
g. have terms and conditions approved by its governing body for the use of its service by payers and beneficiaries. The terms and conditions must be lawful, objective, non-discriminatory and proportionate;
h. ensure that contractual agreements with beneficiaries and the terms and conditions for payers clearly state that a party responsible for a fraudulent or unauthorised or incorrectly issued electronic funds transfer credit payment instruction must bear the risk;
i. demonstrate to the SARB that it has the necessary processes and systems in place to secure the payer's data and online banking credentials to mitigate risks of fraud and cyberattacks;
j. not enter into contractual arrangements with beneficiaries that conduct illegal business; and
k. where is not acting as a beneficiary, perform due diligence on beneficiaries prior to entering into contractual arrangements and on an ongoing basis;
l. due diligence must include at least the following:
    i. verification of the true identity of the beneficiary;

ii. establishment of whether the beneficiary's business is legal and/or registered with the relevant authorities;
iii. understanding the business activity of a beneficiary;
iv. regular monitoring of a beneficiary's transactions for any irregularities; and
v. keeping information obtained for the purpose of establishing and verifying the identities of beneficiaries in line with section 5.3.7.1.

5.2.2 The SARB reserves the right to decline an application for registration if the requirements in this directive are not met. Where an application is declined, the SARB shall disclose reasons for declining the application to the applicant.

5.3 Ongoing obligations

5.3.1 Marketing

5.3.1.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:
a. apply responsible marketing practices on its product or service to payers in a manner that is not fraudulent or likely to create a misleading or false statement; and
b. refrain from using any clearing system participant's branding on its front-end interface or when marketing its services unless it is authorised in writing by the said clearing system participant.

5.3.2 Consumer awareness

5.3.2.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:
a. where it has contracted with a clearing system participant to issue electronic funds transfer credit payment instruction on behalf of the payer, inform its payers and beneficiaries explicitly and clearly of such a contract;

b. publicly disclose, in simple language, terms and conditions for using its product or service, procedures for handling payer complaints, privacy policy and other terms and conditions; and
c. refrain from misleading payers that transactions are compliant with standards that are not applicable to electronic funds transfer credit payments.

5.3.3 Informed consumer consent

5.3.3.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must obtain and receive informed consent prior to using the payer's online banking credentials to access the transactional accounts of the payer to issue an electronic funds transfer credit payment instruction on behalf of the payer.

5.3.3.2 The request for informed consent by the person issuing electronic funds transfer credit payment instructions on behalf of the payer must:
a. be simple and clear to the payer;
b. state that the payer's login credentials will be processed and safeguarded in accordance with applicable information and data privacy legislation;
c. state that electronic funds transfer credit payments are final and irrevocable and that the payer cannot reverse a transaction;
d. state that by entering their login credentials, the payer is sharing the credentials with that person and is not logging on to their online banking website or application;
e. state how the payer's credentials will be safeguarded and protected while in transit and when issuing an electronic funds transfer credit payment instruction; and
f. state that the payer is authorising that person to use their online banking credentials to issue the electronic funds transfer credit payment instruction on their behalf and that such details shall be used only for that purpose.

5.3.3.3 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must request and receive the payer's informed consent to share their login credentials for each electronic funds transfer credit payment instruction, including scheduled payment transactions.

5.3.4 Operational risk

5.3.4.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have sound and effective policies, systems and procedures to mitigate operational risks, including the risks it directly bears from or poses to beneficiaries, its customers, clearing system participants facilitating or enabling electronic funds transfers and/or any other relevant entities;
b. have mechanisms to promptly respond to, resolve and remedy any data breaches, transmission errors, unauthorised access and fraud;
c. have a comprehensive cyber-incident management plan approved by the IT function and its governance structures;
d. the cyber-incident management plan must include promptly informing payers when their online banking credential have been compromised; and
e. carry out regular and comprehensive security risk assessments of its critical staff, IT systems and business process environment to identify, assess and mitigate inherent risk exposures.

5.3.5 Payer data protection

5.3.5.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. 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;
b. issue an electronic funds transfer credit payment instruction on behalf of the payer after the payer has provided informed consent and not modify

any information on the payment instruction unless the payer has provided informed consent;

c. encrypt the payer's online banking credentials at the time when the payer enters the credentials on its front-end interface platform;
d. use the recognised and most robust industry encryption standards to secure the payer's credentials in transit;
e. use and regularly update anti-virus software to protect its system from malware and data security breaches;
f. not store payers' online banking credentials and other sensitive payer payment data within its database or systems;
g. only use the online banking credentials for issuing an electronic funds transfer credit payment instruction on behalf of the payer and safely destroy the payer's online banking credentials immediately after executing a payment; and
h. have adequate information and data security infrastructure and systems to prevent, detect and resolve any possible unauthorised access to the online banking of the payer and/or data breach.

5.3.6 Dispute resolution mechanism

5.3.6.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have a fair and formal dispute resolution mechanism that provides beneficiaries, clearing system participants and payers with practical means to lodge and resolve disputes relating to the issuing of electronic funds transfer credit payment instructions on behalf of the payer, including but not limited to instances of fraud, failure by beneficiaries to honour purchase orders, unpaid orders or failed payments after the beneficiary has already delivered the goods/services and possible data breaches;
b. ensure that its dispute resolution mechanism, including the complaints handling facility is clearly and easily accessible to payers and beneficiaries through all applicable communication channels such as a phoneline, 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.

5.3.7 Traceability, audit and record keeping

5.3.7.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have systems that ensure that each transaction is traceable, from authorisation using the payer's online banking credentials until the beneficiary is notified of the payment;
b. have a robust internal and external audit function that will undertake an assessment of the effectiveness of that person's risk-management and control processes;
c. be able to demonstrate, when requested by the SARB, that it applies robust data security standards, including its data encryption;
d. keep the information obtained during its on-boarding process pertaining to a beneficiary or prospective beneficiary throughout its business relationship and for at least five years from the date on which the business relationship is terminated;
e. keep a record of every transaction, including the payer's informed consent, whether the transaction is a once-off transaction or repeated transaction for at least five 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; and
f. report suspicious and unusual transactions to the Financial Intelligence Centre as per section 29 of the FIC Act.

5.3.8 Liability risk management

5.3.8.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. have an insurance or guarantee mechanism against possible losses for payers and beneficiaries resulting from fraud and refunds;
b. not mislead payers or beneficiaries in believing that the issued electronic funds transfer credit payment instruction will be credited instantly to the beneficiary's account unless the real-time payment option is used to process the payment directly into the beneficiary's transactional account or a transaction is an intrabank transaction processed directly into the beneficiary's transactional account;
c. have an effective mechanism to detect and identify incidents of fraudulent or unauthorised or incorrectly issued electronic funds transfer credit payment instructions and conduct reviews of audit trails to identify the source of the incident to determine the party liable for losses;
d. prove that, where a payer denies having authorised a payment instruction, the informed consent or authorisation was obtained from the payer, with the accurate payment amount and accurate beneficiary name and transactional account number and that the payment was not affected by technical deficiencies within its systems; and
e. pay a refund where it bears the liability or responsibility for fraudulent, unauthorised or incorrectly facilitated transactions to the payer within a reasonable time through the original method of payment, unless specifically agreed by the payer to have the credit processed through an alternate mode.

5.3.9 Attestation of compliance

5.3.9.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must have an audit function or appoint a qualified internal auditor to attest to the declaration of compliance with this directive in the manner and form prescribed by the SARB.

5.3.9.2 The attestation of compliance referred to in paragraph 5.3.9.1 must be submitted to the SARB by 31 March and 30 September each year using the following email address: npsdirectives@resbank.co.za.

5.3.10 Reporting requirements

5.3.10.1 A person issuing electronic funds transfer credit payment instructions on behalf of the payer must:

a. submit to the SARB its monthly data on volumes and values of transactions processed on or before the 15th of every month, using the email address in paragraph 5.3.9.2; and
b. report data security incidents (data breach, cyberattack, fraud and other related types of incidents) to the SARB immediately after being made aware of such incident and provide an analysis of the root cause and preventive measures undertaken to prevent recurrence, using the email address in paragraph 5.3.9.2.

5.3.10.2 The information provided in terms of paragraph 5.3.10.1 will be processed in accordance with section 33 of the SARB Act and section 10 of the NPS Act.

6. Supervision and compliance monitoring

6.1 A representative of the SARB may conduct a supervisory on-site or off-site inspection on the person issuing electronic funds transfer credit payment instructions on behalf of the payer, to promote compliance with this directive.

6.2 Subject to paragraphs 6.5.3 and 6.5.4, the SARB must provide prior written notification to the person whose business premises will be inspected.

6.3 The supervisory on-site inspection notification will specify:

6.3.1 date(s) of the intended supervisory on-site inspection;
6.3.2 names of the SARB representatives;
6.3.3 period under review; and

6.3.4 any other information/documentation required for inspection purposes.

6.4 Each SARB representative must produce a letter of authority and an identity document upon entry at the premises of a person issuing electronic funds transfer credit payment instructions on behalf of the payer, which officials must view for verification purposes and are prohibited to produce copies thereof.

6.5 The SARB representatives may enter any premises:

6.5.1 without prior consent in the case of business premises operated by a person issuing electronic funds transfer credit payment instructions on behalf of the payer; or

6.5.2 with prior consent:

6.5.2.1 in the case of a private residence, where the business of the person issuing electronic funds transfer credit payment instructions on behalf of the payer is reasonably believed to be conducted at the private residence; or

6.5.2.2 in the case of persons not registered to issue electronic funds transfer credit payment instructions on behalf of the payer after informing that person that:

a. granting consent will enable the SARB representative to enter the premises and for the SARB to subsequently search the premises; and
b. he or she is under no obligation to admit the SARB representative in the absence of a warrant; or

6.5.3 without prior consent and without prior notice to any person issuing electronic funds transfer credit payment instructions on behalf of the payer if the entry is authorised by a warrant in terms of paragraph 6.16; or

6.5.4 with the prior authority of a senior staff member of the SARB, if the senior staff member on reasonable grounds believes that:

6.5.4.1 a warrant will be issued if applied for, in terms of paragraph 6.16;

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

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

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

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

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

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

6.6.4 require a person on the premises to produce to the SARB representatives any document or item that is relevant to the investigation and is in the possession or under the control of the person;

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

6.6.5.1 search any information in or available through that system; and

6.6.5.2 produce a record of that information in any format that the SARB representatives reasonably require;

6.6.6 if it is not practicable or appropriate to make a requirement in terms of subparagraph 6.6.5, operate any computer or similar system on or available through the premises for a purpose set out in that subparagraph; and

6.6.7 take possession of, and take from the premises, a document or item that may afford evidence of a contravention of this directive or may be relevant to the inspection.

6.7 The SARB 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 6.6.

6.8 Subject to paragraph 6.9, the SARB representative must ensure that any document or item taken by the SARB representative as mentioned in paragraph 6.6 is returned to the person when:

6.8.1 retention of the document or item is no longer necessary to achieve the object of the inspection; or

6.8.2 all proceedings arising out the inspection have been finally disposed of.

6.9 A document or item need not be returned to the person who produced it if:

6.9.1 the document or item has been handed over to a designated authority; or

6.9.2 it is not in the best interest of the public or any member or members of the public for the documents or items to be returned.

6.10 A person from whose premises a document or item was taken as mentioned in paragraph 6.6, or its authorised representative, may, during normal office hours and under the supervision of a representative of the SARB, examine, copy and make extracts from the document or item.

6.11 A person who is questioned, or required to produce a document or information during a supervisory on-site inspection contemplated, may object to answering the question or to producing the document or the information on the grounds that the answer, the contents of the document or the information may tend to incriminate the person.

6.12 On such an objection, the SARB representative conducting the supervisory on-site inspection may require the question to be answered or the document or information to be produced, in which case the person must answer the question or produce the document.

6.13 An incriminating answer given, and an incriminating document or information produced, as required in terms of paragraph 6.12, is not admissible in evidence against the person in any criminal proceedings, except in criminal proceedings for perjury or in which that person is tried based on the false or misleading nature of the answer.

6.14 The SARB representative conducting a supervisory on-site inspection must inform the person of the right to object at the commencement of the supervisory on-site inspection.

6.15 A judge or magistrate who has jurisdiction may issue a warrant for the purposes of this paragraph on application by a representative of the SARB.

6.16 The judge or magistrate may issue a warrant in terms of this paragraph:

6.16.1 on written application by the SARB setting out under oath or affirmation why it is necessary to enter and inspect the premises; and

6.16.2 if it appears to the magistrate or judge from the information under oath or affirmation that:

6.16.2.1 there are reasonable grounds for suspecting that a contravention of the directive has occurred, may be occurring or may be about to occur;

6.16.2.2 entry and inspection of the premises is likely to yield information pertaining to the contravention; and

6.16.2.3 entry and investigation of those premises is reasonably necessary for the purposes of the investigation.

6.17 A warrant issued in terms of this paragraph must be signed by the judge or magistrate issuing it.

6.18 SARB representatives that enter the premises under the authority of a warrant must:

6.18.1 if there is apparently no one 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

6.18.2 on reasonable demand by any person on the premises, produce the warrant or a copy of the warrant.

7. Effective date and non-compliance

7.1 The directive is effective 90 days after publication thereof. The SARB reserves the right to amend any requirements in this directive.

7.2 A person issuing an electronic funds transfer credit payment instruction on behalf of the payer must comply with the requirements or conditions as stipulated in this directive.

7.3 Contravention of this directive is an offence in terms of section 12(8) of the NPS Act.

7.4 The SARB may terminate the registration of a person registered in terms of this directive where such person fails to comply with this directive, or if it is in the interest of the safety and efficiency of the NPS. Any person whose registration has been terminated shall immediately cease to issue electronic funds transfer credit payment instructions on behalf of any payer.

7.5 Prior to terminating a registration, the SARB shall issue a notice of its intention to terminate the registration and give that person reasonable time to remediate the deficiencies identified. The time provided to remediate the deficiencies shall be determined on a case-by-case basis.

8. Conclusion

8.1 If a person issuing an electronic funds transfer credit payment instruction on behalf of the payer is uncertain as to whether its current or future business practices are aligned with this directive, that person should initiate discussions with the SARB to clarify the matter.

8.2 Attestation of compliance as well as any enquiry or clarification concerning this directive should be sent to the following email address: npsdirectives@resbank.co.za.