DIRECTIVE IN ACTION: SARB'S PUSH TO FORTIFY SOUTH AFRICA'S PAYMENT INFRASTRUCTURE

Category: Privacy Law and POPIA,Technology Law
written by Tshimangadzo Nengovhela | September 15, 2025

The South African Reserve Bank ("**SARB**"), under the authority granted by the SARB Act 90 of 1989 and the National Payment System Act ("**NPS Act**"), plays a vital role in the regulation and oversight of payment, clearing, and settlement systems within South Africa. This responsibility lies with the SARB's National Payment System Department ("**NPSD**").

The National Payment System ("**NPS**") is integral to the country's financial infrastructure, facilitating secure and efficient monetary circulation from payer to beneficiary. As the payment landscape evolves with increasing digitisation, fintech adoption, and reliance on third-party IT services, the risk of cybersecurity threats also escalates. Recognising these growing threats, SARB issued a comprehensive Cybersecurity and Cyber-Resilience Directive applicable to payment institutions, system operators, and financial market infrastructures ("**FMIs**"). This directive ensures the integrity, efficiency, and security of the NPS against cyber incidents that could cause systemic disruptions.

Purpose of the Directive

SARB, exercising its authority under section 12 of the NPS Act, introduced this directive to enforce

cybersecurity and cyber-resilience obligations on all stakeholders in the payment ecosystem. The directive outlines minimum requirements and best practices for:

- Governance
- Cyber-risk identification
- Prevention and detection
- Response and recovery
- Testing and reporting
- Regulatory compliance

Who Must Comply

This directive applies to:

- Payment Institutions
- Operators
- Payment System Financial Market Infrastructures

Cyber Governance Frameworks

Institutions are required to establish comprehensive written governance frameworks that define their cyber objectives and risk tolerance. These frameworks must include the appointment of qualified executives responsible for cybersecurity and ensure alignment between cyber-resilience strategies and broader business continuity and operational risk plans. Board oversight is essential, with mandated annual reviews of cyber policies. Additionally, institutions must foster collaboration with SARB and other relevant stakeholders to strengthen cyber governance.

Critical Asset Identification

Institutions must identify and classify their critical operations, technologies, and data assets. This includes mapping external dependencies and access rights, as well as understanding cyber-risk interconnections within the National Payment System. Proper classification ensures that institutions can prioritize protection and response efforts effectively.

Cybersecurity Measures

A robust, risk-based cybersecurity framework is essential. It should incorporate protective controls such as multi-factor authentication and encryption, alongside secure design principles for payment services. Regular employee training is required to maintain awareness and preparedness. Institutions must also comply with industry standards and implement cyber hygiene practices, including patch management and malware defences.

Threat Detection

Institutions must deploy multi-layered detection systems capable of identifying and responding to threats. Behavioural analytics should be used to flag irregular access patterns or suspicious activities, enhancing the ability to detect sophisticated cyber threats in real time.

Incident Response and Recovery

Institutions are expected to restore critical operations within a timeframe of 2 to 8 hours – depending on the classification of the affected systems. They must maintain documented and regularly tested response plans. Furthermore, institutions should assess and monitor the cyber capabilities of third-party providers, address risks associated with cloud service providers and ensure accountability across all service relationships.

Cyber-Resilience Testing

Cyber-resilience frameworks must include scenario-based simulations to test preparedness for various threat scenarios. Penetration testing – both internal and external – is required, along with vulnerability assessments following significant system changes. These practices help institutions identify and address weaknesses before they can be exploited.

Information Sharing

Institutions have an obligation to share cyber threat intelligence with SARB and relevant industry groups. Participation in recognised information-sharing bodies, such as the Cybersecurity Hub, is encouraged. All information-sharing activities must comply with data protection laws, including the Protection of Personal Information Act and the Cybercrimes Act.

Situational Awareness

Maintaining situational awareness is critical. Institutions must stay informed about the evolving cyber-threat landscape and develop capabilities for gathering and analysing cyber-threat intelligence. Understanding threats within the broader NPS ecosystem is essential for proactive risk management.

Learning and Evolving

Cybersecurity frameworks must be adaptable and forward-looking. Institutions should learn from past incidents and continuously evolve their strategies. Incorporating predictive and proactive threat management techniques ensures resilience against emerging cyber risks.

In the event of a material cyber incident, payment institutions and operators are required to report the incident to SARB within 24 hours. A detailed follow-up report must be submitted within 48 hours. The report mustoutline the cause of the incident, its impact, recovery plans, and any potential systemic effects. Institutions must also provide regular updates throughout the incident response process and submit a comprehensive post-incident remediation report to ensure accountability and continuous improvement.

Supervision and Compliance Monitoring

To ensure adherence to the directive, SARB may conduct onsite or offsite inspections at any time. These inspections can be scheduled with prior written notice or carried out without notice in cases of urgency or under judicial warrant. SARB officials are authorised to access documents and systems, question staff, and copy, examine, or seize any documents relevant to the inspection. While individuals may object to providing self-incriminating information, they may still be compelled to respond under specific legal conditions.

Effective Date and Enforcement

The directive will take effect three months after its publication. Non-compliance constitutes an

offence under section 12(8) of the National Payment System Act. SARB retains the authority to amend the directive's requirements as necessary to respond to evolving risks and regulatory needs.

Conclusion and Contact

This directive marks a critical advancement in strengthening cyber resilience across South Africa's financial ecosystem. It recognizes the rapidly changing threat environment and sets out clear, enforceable obligations for all stakeholders within the NPS. For further enquiries, institutions may contact SARB via email at: NPSDIRECTIVES@resbank.co.za.