VERSO®

Umbrella Retirement Provident Fund

# Legal & industry update: September 2026

**In this publication we look at:**

- FSCA-PA Joint Communication 5 of 2026 and Joint Notice 2 of 2026 – the templates and turnaround times when reporting material IT or cyber incidents; and
- National Treasury's Framework to Centralise Unclaimed Financial Assets in South Africa

## FSCA-PA Joint Communication 5 of 2026 & Joint Notice 2 of 2026 - Reporting material IT or cyber incidents

From 1 September 2026, retirement funds must use the prescribed reporting template and the FSCA's Joint Standards Submission Portal when notifying the Financial Sector Conduct Authority (FSCA) of a material IT or cyber incident.

### *A staged incident-reporting process*

The immediate challenge for trustees of retirement funds is to make sure their incident management arrangements can support a three-stage reporting process. A material incident must be reported to the FSCA through the **Joint Standards Submission Portal** using the prescribed **Reporting of Material IT and/or Cyber Incident Template.**

The timetable is demanding:

| Reporting stage | Deadline | Practical focus |
|---|---|---|
| Immediate notification | Within 24 hours after classification as a material incident | Notify the FSCA promptly with the information available |
| Subsequent update | Withing 14 calendar days of the FSCA notification | Set out developing impact, investigation findings and remedial action |
| Full incident report | Within timeframe agreed with the FSCA | Submit the completed template and final investigation report |

The key point is that the 24-hour clock starts when the fund classifies an incident as material, not when the event is first detected. It is also a 24-hour period, rather than 24 business hours. Funds therefore need a process that can bring the right people together quickly including the principal officer, relevant trustees, administrator, IT and cybersecurity providers, legal advisers and communications teams to reach and document a materiality decision.

This is not simply a technology issue. A cyber incident can include a breach of security policies, procedures or acceptable-use rules, whether malicious activity or an external attack was involved. For example, an employee's improper disclosure of member data could fall within the cyber-incident framework even if no system was hacked or technical security setting altered. The fund must then separately assess whether the incident was material.

Materiality remains a principles-based determination for the fund, considering its nature, size, complexity and risk profile. The relevant question is whether a disruption has had, or is likely to have, a severe and widespread effect on operations, member or beneficiary services, or the wider financial system and economy.

For trustees, this calls for a practical decision framework. It should prompt consideration of the actual or likely impact on member and beneficiary data, contribution processing, benefit calculations and payments, member service availability, system integrity, third party dependencies and the duration and scale of any disruption. The aim is not to wait for perfect information, but to make a reasoned decision on the facts available and update it as the investigation progresses.

## Trustees remain accountable

Outsourcing does not delegate regulatory responsibility. Although many retirement funds depend on administrators and other service providers for core systems, cyber controls and operational processing, the board of trustees remains ultimately accountable for the fund's compliance.

An administrator's report to a regulator cannot serve as a proxy for the fund's own reporting obligation.

That makes contractual readiness essential. Service level agreements should require providers to:

- identify, contain and escalate relevant incidents to the fund without delay,
- provide sufficient information for the fund's materiality assessment,
- preserve evidence,
- cooperate with the investigation, and
- support the fund's regulatory submissions and member communications.

The initial report may necessarily contain gaps. Where the template allows an "unknown" response, funds should use it where accurate, submit on a best-efforts basis and provide further or corrected information through the later reporting stages. They should not treat the initial notification as a document to be repeatedly amended. Equally, an FSCA submission does not replace separate notification duties under POPIA or other applicable laws. Each regulator's requirements must be considered independently.

A sensible governance response is to run incident simulations before a crisis. Trustees should know:

- who has authority to classify an incident as material,
- who submits the notification,
- how after-hours escalation works,
- how decisions are recorded and
- how the fund obtains confirmation that the FSCA portal submission has been received.

## National Treasury's unclaimed financial assets proposal

National Treasury's proposed framework on unclaimed assets signals a potentially significant redesign of how unclaimed retirement benefits, and eventually other dormant financial assets dispersed across banks, insurers and investment providers, are held, traced and paid.

The proposal responds to fragmented definitions, uneven tracing practices, inconsistent record keeping and the difficulty consumers face when trying to establish whether they have an unclaimed entitlement.

The proposed model would centralise custody and investment of qualifying unclaimed assets through the Corporation for Public Deposits (CPD), while a central unclaimed financial assets administrator would maintain the consolidated dataset, coordinate tracing, administer individual records and process claims. National Treasury envisages a single public facing portal through which owners and beneficiaries could search, enquire and track claims.

For retirement funds, the Pension Funds Act already provides an important starting point: a benefit that has been legally due and payable but remains unpaid for 24 months is treated as unclaimed, after tracing efforts have resulted in the member not being found. Treasury proposes beginning the centralisation programme with unclaimed retirement benefits before extending it to dormant bank accounts, insurance proceeds and investment products.

The attraction is clear. A central model could standardise data fields, tracing practices, service standards, record retention and claims processing. It could also reduce duplication, improve matching against authorised datasets and make it easier for members and beneficiaries to locate benefits that have become separated from them through job changes, outdated contact information or incomplete records.

## The difficult policy choices

The proposal does not mean that the state would immediately take ownership of unclaimed benefits. Under the contemplated CPD model, the assets would continue to be held for owners and beneficiaries, with valid claims paid from the net balance of the relevant account. The CPD's role would be custody and investment within its legal mandate; the administrator's role would be tracing, records and claimant service.

However, Treasury has raised a more difficult question: should there ultimately be a statutory cut-off after which an asset can no longer be claimed? Two options are canvassed:

- An asset would cease to be claimable when the owner reaches, or would have reached, age 110.
- An asset would cease to be claimable 45 years after it first became unclaimed.

National Treasury argues that a limit could create legal certainty, encourage earlier claims and avoid the cost of preserving records and conducting tracing indefinitely. The 45-year option is presented as more administratively efficient because it is based on an objective date rather than the owner's age.

This will be a sensitive consultation issue for the retirement fund industry. Any final framework will need to balance administrative practicality against the fundamental principle that retirement benefits are intended for members and their beneficiaries. It will also need robust safeguards around data security, POPIA compliance, authentication, audit trails, fee transparency and the integrity of transferred records.

Responses on the proposed framework are due by 19 September 2026.



Verso Umbrella Retirement Provident Fund • Belmont Office Park • Twist Street • Bellville • 7530 • P O Box 4300 • Tyger Valley • 7536 • Tel: 087 330 2001 • E-mail: info@vurf.co.za • www.vurf.co.za • Registration no. 12/8/37308