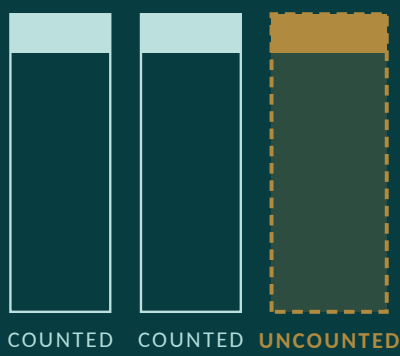
01

The three weeks nobody counts

Dwell time, and the interval that financial-sector controls and disclosures were never designed to measure.

Series premise: what goes unmeasured tends to go unmanaged.



Two kinds of attacker are counted. A third is not.

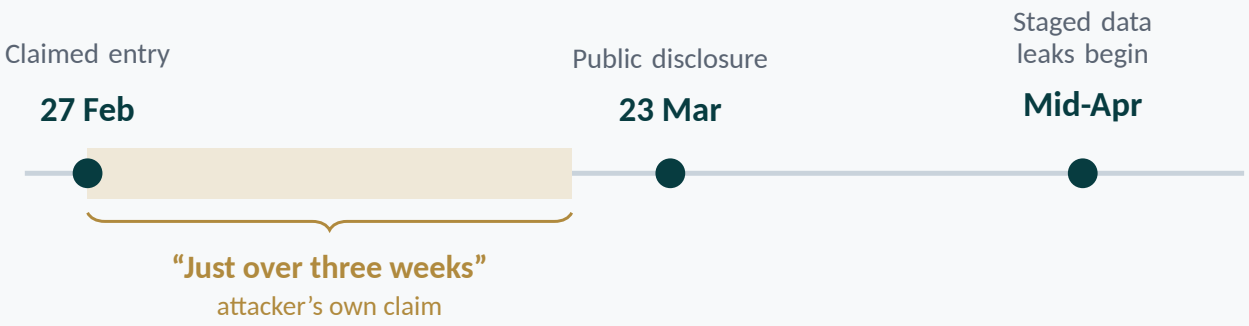
South Africa's banks already publish two prevented-loss figures: fraudulent applications stopped at onboarding, and scam payments stopped by behavioural scoring. Both appear at results because the industry has agreed they are worth counting.

A third kind of exposure passes both checks, largely because much of it never becomes a payment. With no transaction to reverse, there is no loss line to report, and so no figure.

Onboarding checks	Payment-behaviour scoring	The uncounted
CATCHES	CATCHES	THIS PART
A false application	A deceived client	**Time spent inside before anyone knows**
R7.5bn blocked Nedbank, 2024[7]	R673m avoided Capitec, FY2026[8]	No equivalent figure published
Measured & disclosed	Measured & disclosed	No published figure

This series examines four places where that gap has become visible in 2026. Part 1 concerns time.

What has been reported about the Standard Bank incident



Standard Bank and its subsidiary Liberty disclosed data breaches on 23 March 2026.[1] A threat actor calling itself ROOTBOY later claimed to have entered on 27 February and to have remained undetected for just over three weeks, exfiltrating some 1.2 TB of data.[2]

The bank has said that the affected systems were internal administrative and document-filing systems, and that in a limited number of cases card numbers and expiry dates were included, though not CVVs.[2,3]

The duration is the attacker's claim and has not been independently verified. The incident is used here because its disclosures are public, not to single out the institution.

Weeks inside, and not a single payment

By the attacker's own account, the time was spent moving through collaboration, service-management and database platforms.[4] None of these is a payment system, and none of that movement would have registered as a transaction.

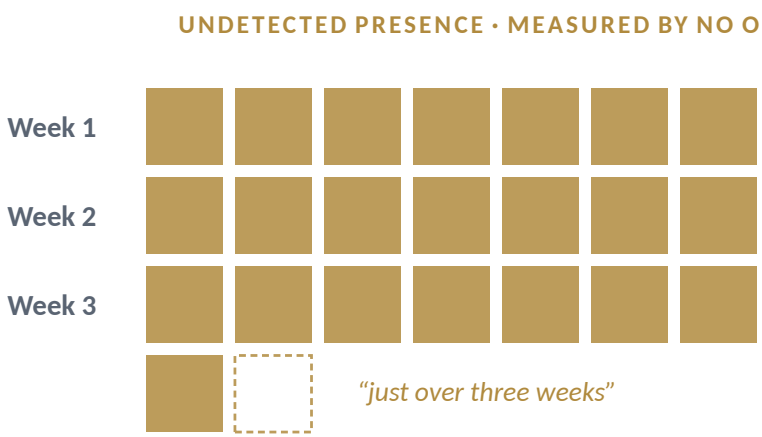
This is precisely the activity that the two measured controls are not built to observe. Onboarding checks had long since approved the accounts in use, and payment scoring had nothing to score, so each control performed as designed while the intrusion continued.

> **THE MEASUREMENT PROBLEM**
>
> An incident of this kind produces a disclosure and, eventually, a remediation cost. It does not produce a prevented-loss figure, because there was no payment to prevent, and so the period in which the exposure was actually incurred remains largely absent from the numbers the sector reports.

Three weeks, against one day

Joint Standard 2 of 2024, binding on banks since 1 June 2025, requires material cyber incidents to be reported within 24 hours.[5] That clock starts when an incident is classified as material, which can only happen once it has been identified.

DRAWN TO SCALE · ONE SQUARE IS ONE DAY



REPORTING WINDOW

24 h

Runs from classification as material, never from entry. Regulated to the hour.

The duration shown is the attacker's claim; the bank has not disclosed one. The proportion is the point: the part of the incident the framework governs is one square.

The framework governs the final day with some precision. The weeks that precede it, during which most of the exposure is incurred, fall outside any figure an institution is currently asked to publish.

Questions worth asking before an incident, not after

1. On our most recent incident involving valid access, how long elapsed between entry and identification, and by what means was it eventually found?

2. Do we measure dwell time at all, and if so, is it reported to the board alongside the fraud and loss figures we already track?

3. Which of our internal systems (collaboration, ticketing, document stores) hold client data, and does anything observe how that data is accessed when no payment is involved?

4. Were an attacker to remain inside for three weeks, what would they be able to read, and for how long would that information retain its value?

Uncertainty about the answer to any of these is itself a measure of the exposure.

THE POINT

Dwell time is a governance metric

The industry has become skilled at counting what it prevents at the moment of payment. The difficulty is that a growing share of exposure is incurred well before that moment, and in systems that never touch a payment at all.

Treating the interval between entry and identification as something to be measured, reported and reduced, in the same way that application fraud and scam losses already are, would bring the uncounted part of the problem into the same governance conversation as the counted one. The absence of a figure has, for too long, been read as the absence of a problem.

> NEXT IN THE SERIES
>
> Part 2 — One provider, many perimeters. What a single third-party incident reveals about where responsibility ends and exposure concentrates.

Sources, and how each is used

Company, regulator and industry-body publications are cited directly wherever they exist. Press reports are used where they are the only public record, chiefly for client notices not otherwise published and for claims made by threat actors, and are marked as such.

1 COMPANY Standard Bank, “An important data incident update”, 23 March 2026, and update of 14 April 2026, standardbank.co.za; Liberty disclosure of 24 March 2026.

2 PRESS · CLAIM MyBroadband, “1.2TB of Standard Bank data, including credit card details, stolen and leaked online”, April 2026. Entry date, duration and data volume are the threat actor’s claims.

3 PRESS MyBroadband, “Standard Bank sends warning to customers about stolen credit card details”, April 2026; Daily Maverick, 17 April 2026.

4 PRESS · CLAIM Threat actor’s forum statement, as quoted by ITWeb, “Hackers publicly release data stolen from Standard Bank”, April 2026. Not independently verified.

5 REGULATOR FSCA and Prudential Authority, Joint Standard 2 of 2024: Cybersecurity and Cyber Resilience Requirements, effective 1 June 2025; joint determination on notifying material IT and cyber incidents, effective 1 September 2026 (initial notification within 24 hours of classification as material).

6 INDUSTRY BODY SABRIC, Annual Crime Statistics 2025, for the sector’s published digital banking fraud figures referenced in the series premise.

7 COMPANY Nedbank, application-fraud attempts blocked at account opening in 2024, as presented at the SAFPS International Fraud Summit, 2025.

8 COMPANY Capitec Group, results for the year ended February 2026: client losses avoided and fraudulent beneficiaries blocked.