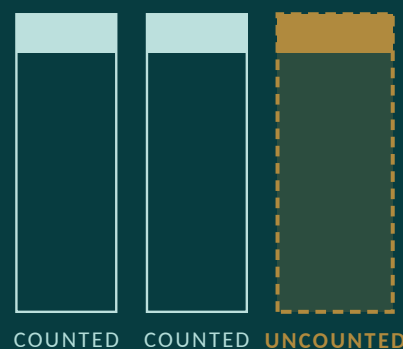


One provider, many perimeters

Third-party concentration, and why an institution's own controls cannot see the environment that now holds its clients' data.

Responsibility is fragmented. Exposure is concentrated.



The gap, seen from outside the perimeter

Part 1 examined time: the weeks an intruder can spend inside before anyone knows. Part 2 examines place, and specifically the environments that sit outside an institution’s estate while holding data the institution is accountable for.

Activity in those environments passes both measured controls by definition, since neither onboarding checks nor payment scoring was ever designed to look beyond the institution’s own systems.

Onboarding checks	Payment-behaviour scoring	The uncounted
CATCHES A false application	CATCHES A deceived client	THIS PART Data held outside the institution’s own estate
Measured & disclosed	Measured & disclosed	No published figure

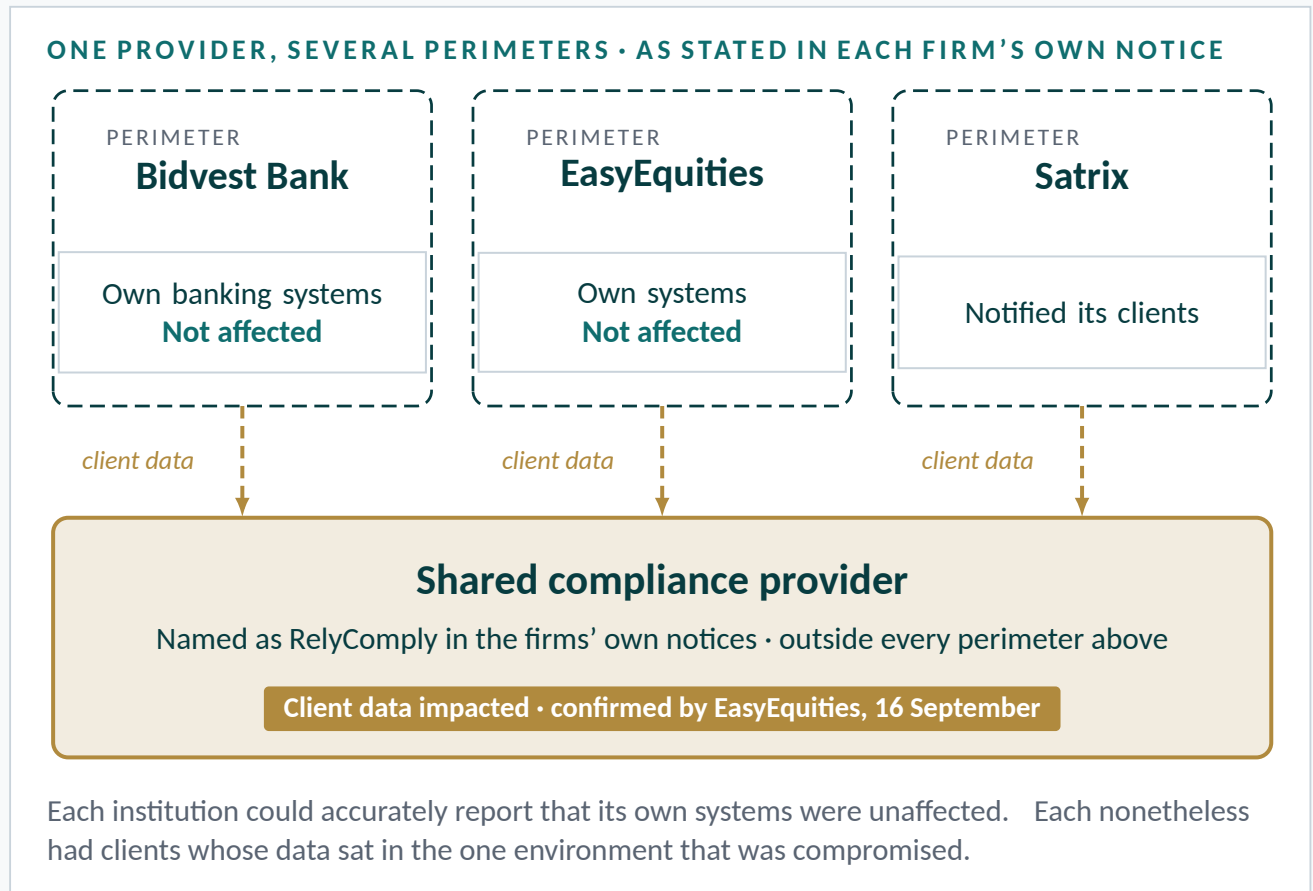
One weekend, several notices, similar wording

In September 2026, Bidvest Bank, EasyEquities and Satrix notified clients of a cyber incident at a third-party service provider.^{1,2} EasyEquities explained that the provider conducts client-verification checks on its behalf, in line with regulatory obligations.² Satrix subsequently identified that provider as the regtech company RelyComply.³

Bidvest Bank's notice of 17 September explains that it uses the provider for anti-money-laundering transaction monitoring and sanctions screening, that its own banking systems were unaffected, and that it is treating personal information in the provider's environment as potentially accessed, since forensic work had not yet established what was taken.¹ EasyEquities later confirmed that client data held by the provider had been impacted, while reporting no evidence of access to its own systems.⁴

Bidvest Bank's notice describes the unauthorised party as understood to be affiliated with the Direwolf group, which listed RelyComply on its leak site on 9 September. RelyComply has since said the access has stopped and that it found no evidence of movement into any customer network, subject to forensic verification.^{1,5,8} Institutions are named only as their own notices name them.

Each perimeter held. The exposure sat between them.



Responsibility for the data remains fragmented across the firms that collected it, whereas the exposure is concentrated in the single environment where it is processed.

Not an isolated arrangement

The same provider's reach extended further than the first notices suggested. Virgin Active's notice of 22 September explains that the provider performed transaction monitoring for its payment provider, Peach Payments, and that the data involved may have included partial card numbers and transaction details.⁸ The exposure sat two contracts away from the firm whose customers it concerned.

Cell C reported an unrelated incident at a different provider in the same month, with the same shape: valid access, in someone else's environment, to someone else's clients' records.^{1,6}

WHY CONTROLS DO NOT SEE IT

An institution's monitoring is scoped to the estate it operates. A credential issued by a provider, used inside that provider's environment, generates no event the institution can observe. The first signal is frequently the provider's own notice.

Outsourcing moves the work. It does not move the accountability, which remains with the institution that collected the data and answers to the Information Regulator for it.

Third-party risk is now a board matter

Joint Standard 2 of 2024 extends its cybersecurity and cyber-resilience requirements to an institution's arrangements with third-party service providers.⁷ In practice, that places the security of a provider's environment within the scope of the institution's own governance, and so within the scope of its board.

The difficulty is that most oversight of providers remains periodic and document-based (questionnaires, certifications, contractual undertakings), whereas the exposure described here is continuous and operational. A provider may be fully compliant on the day of its assessment and compromised on the day after.

THE MEASUREMENT PROBLEM, AGAIN

No institution currently reports how much of its clients' data resides outside its own estate, or how quickly it would learn of a compromise there. Both figures would be uncomfortable to produce. Both would be more useful than their absence.

Questions worth asking this quarter

- 1 Which third parties hold our clients' personal or identity data, including our providers' own providers, and where do several of them depend on the same one?
- 2 How quickly are our providers contractually obliged to tell us of an incident, and how would we learn of one they had not yet detected themselves?
- 3 What assurance do we have over how our providers issue, protect and monitor the credentials that reach our clients' data?
- 4 If a provider's environment were compromised tomorrow, which of our own controls, including onboarding, would we need to treat as weakened?

NEXT IN THE SERIES

Part 3 — The request that looked legitimate. What happens when a process is followed correctly and the request itself is fraudulent.

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** Bidvest Bank, “Notification of a Security Compromise in terms of Section 22 of POPIA”, 17 September 2026 (“RelyComply Cyber Incident – 8 September 2026”), [bidvestbank.co.za](https://www.bidvestbank.co.za); with Connecting Africa, “SA’s Cell C, EasyEquities and Bidvest Bank warn customers of data leak”, September 2026.
- 2 **PRESS** MyBroadband, “EasyEquities informs customers about possible data breach”, September 2026, quoting the Bidvest Bank and EasyEquities notices.
- 3 **PRESS** Moneyweb, “EasyEquities, Satrix hit by data breach”, September 2026; TimesLIVE, “Cyberattacks put South Africans’ personal data in the spotlight”, 15 September 2026.
- 4 **PRESS** MyBroadband, “EasyEquities data at third-party hacked and customer information compromised”, 16 September 2026, quoting EasyEquities’ client notice.
- 5 **PRESS · CLAIM** RedPacket Security and CyPro reporting of the Direwolf leak-site listing, 9 September 2026. An unconfirmed claim. Bidvest Bank’s notice of 17 September describes the party as understood to be affiliated with Direwolf.
- 6 **PRESS** MyBroadband, September 2026: Cell C confirmed its incident related to a different third party.
- 7 **REGULATOR** FSCA and Prudential Authority, Joint Standard 2 of 2024, effective 1 June 2025.
- 8 **COMPANY** Virgin Active, “Cybersecurity incident at RelyComply”, customer notice, last updated 22 September 2026.