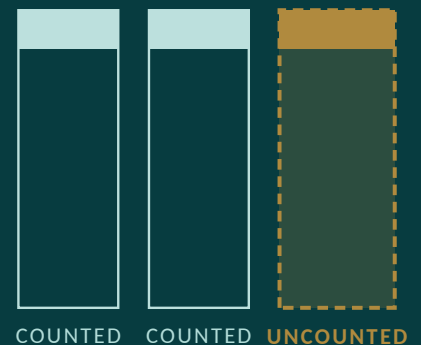


Identity at the source

What happens to onboarding checks once the documents they depend on are themselves in circulation.

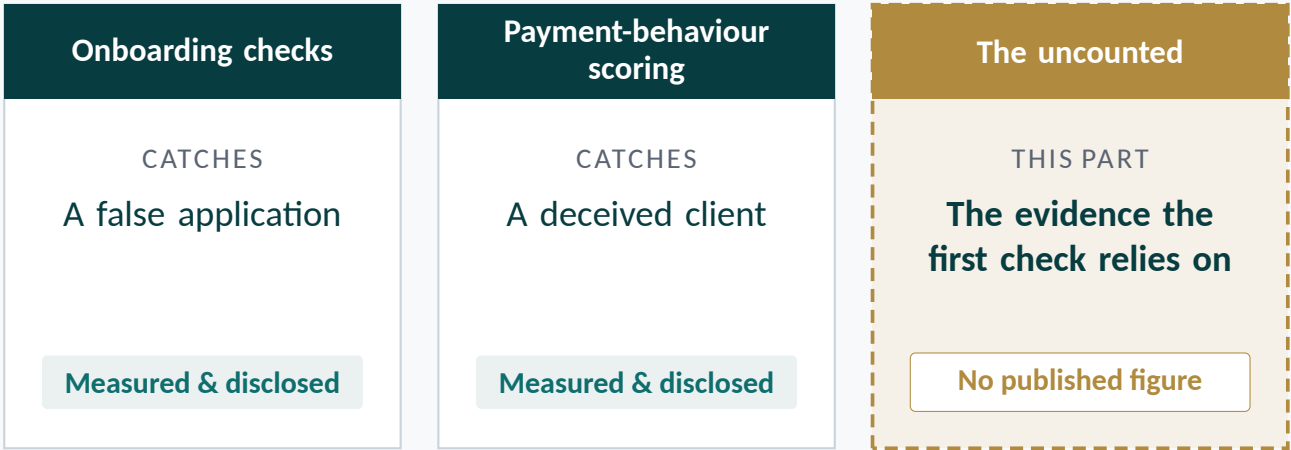
A password can be reset. A face cannot be reissued.



The first measured control, under strain

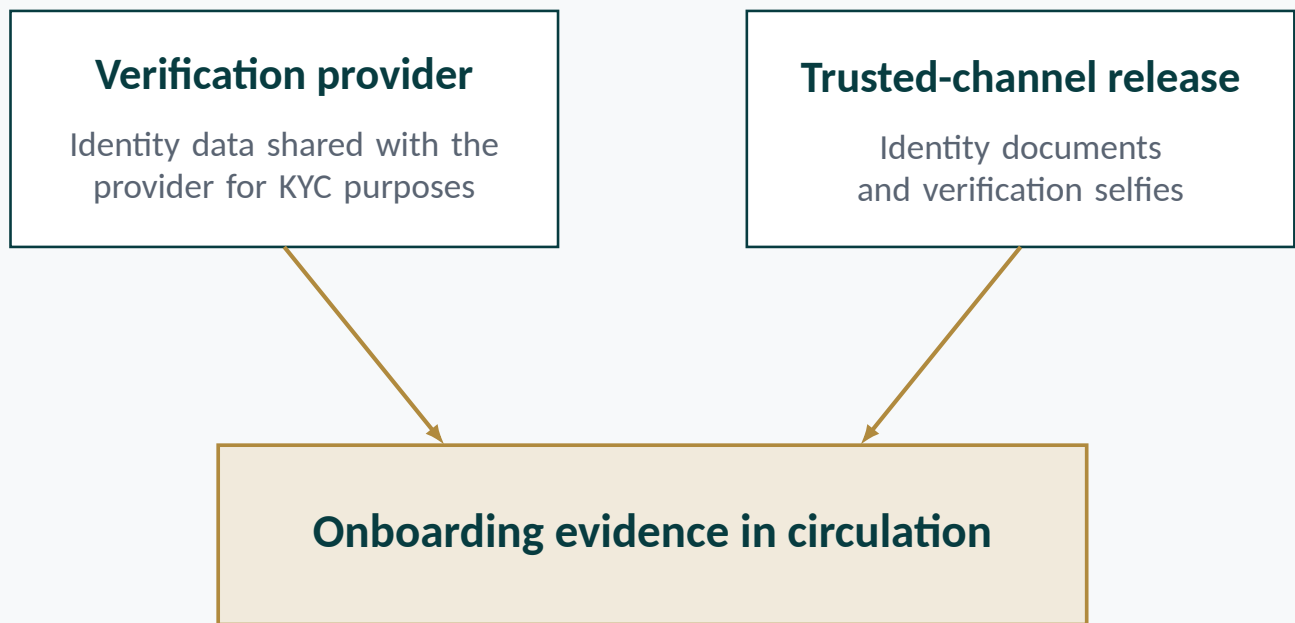
The first three parts examined exposures that pass both measured controls. Part 4 turns to the first of those controls itself, and to a quieter consequence of the incidents already described.

Onboarding checks work by comparing an applicant against identity evidence: an identity document, a verification selfie, supporting records. They remain effective only for as long as that evidence is difficult for someone else to obtain.



Two incidents, one category of data

The incidents in Parts 2 and 3 differed in almost every respect: one involved a verification provider serving several regulated firms,¹ the other a trusted channel at a single fintech.² What they share is the data exposed.



In each case, the material exposed was the material institutions collect specifically in order to establish that a person is who they claim to be.

The check still passes. That is the problem.

When identity evidence circulates, synthetic and borrowed identities become cheaper to assemble. An application built on genuine documents and a genuine likeness does not look false, and so an onboarding check that approves it is performing exactly as designed.

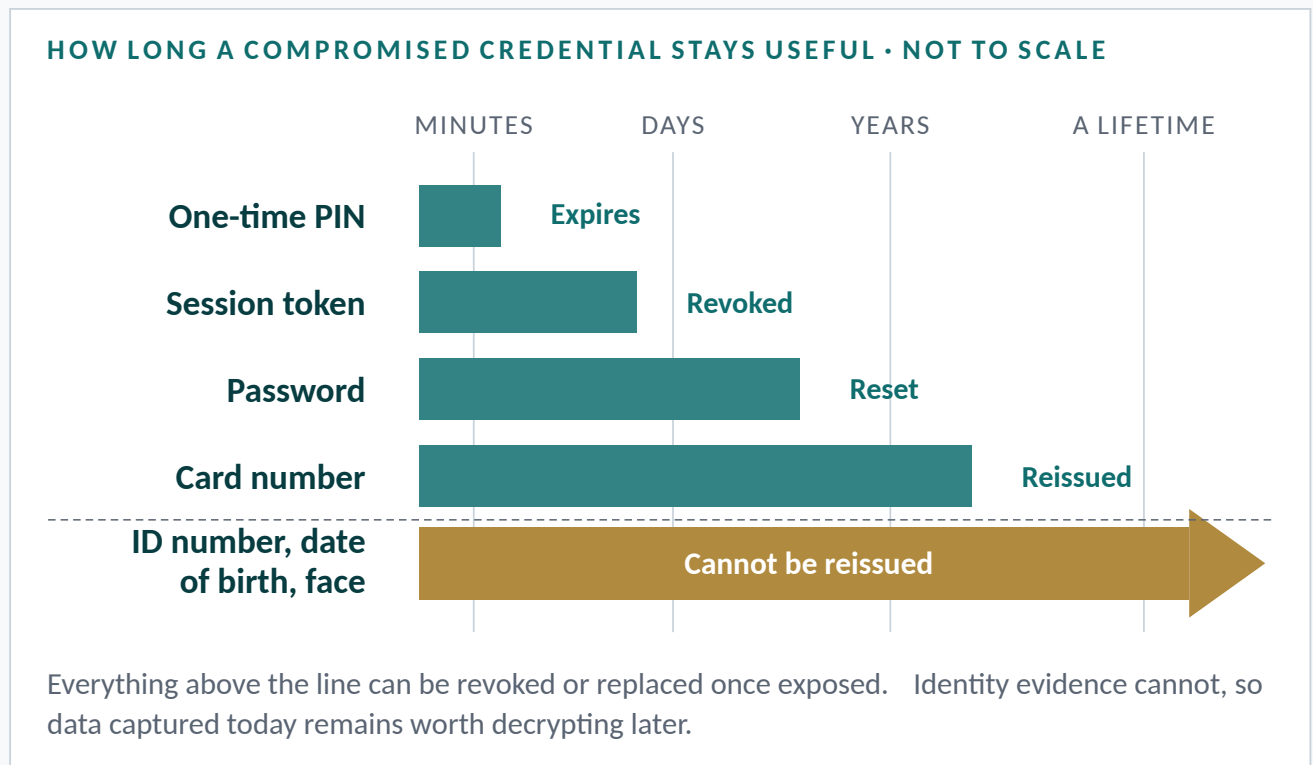
The first measured control therefore weakens without failing, and without any change in the figure it reports. Prevented application fraud may remain impressive while the share of fraudulent applicants who now pass goes, by construction, unobserved.

THE SHIFT THAT FOLLOWS

Weight moves from the moment of onboarding to what happens afterwards: how an account, a credential or an access right actually behaves once it has been granted. That is the one place where a convincing identity cannot, on its own, disguise intent.

The data that outlives the system

Most compromised data can be made worthless. Cards are reissued, passwords reset, tokens revoked. Identity evidence is different: an identity number, a date of birth and a face remain valid for the life of the person they describe.

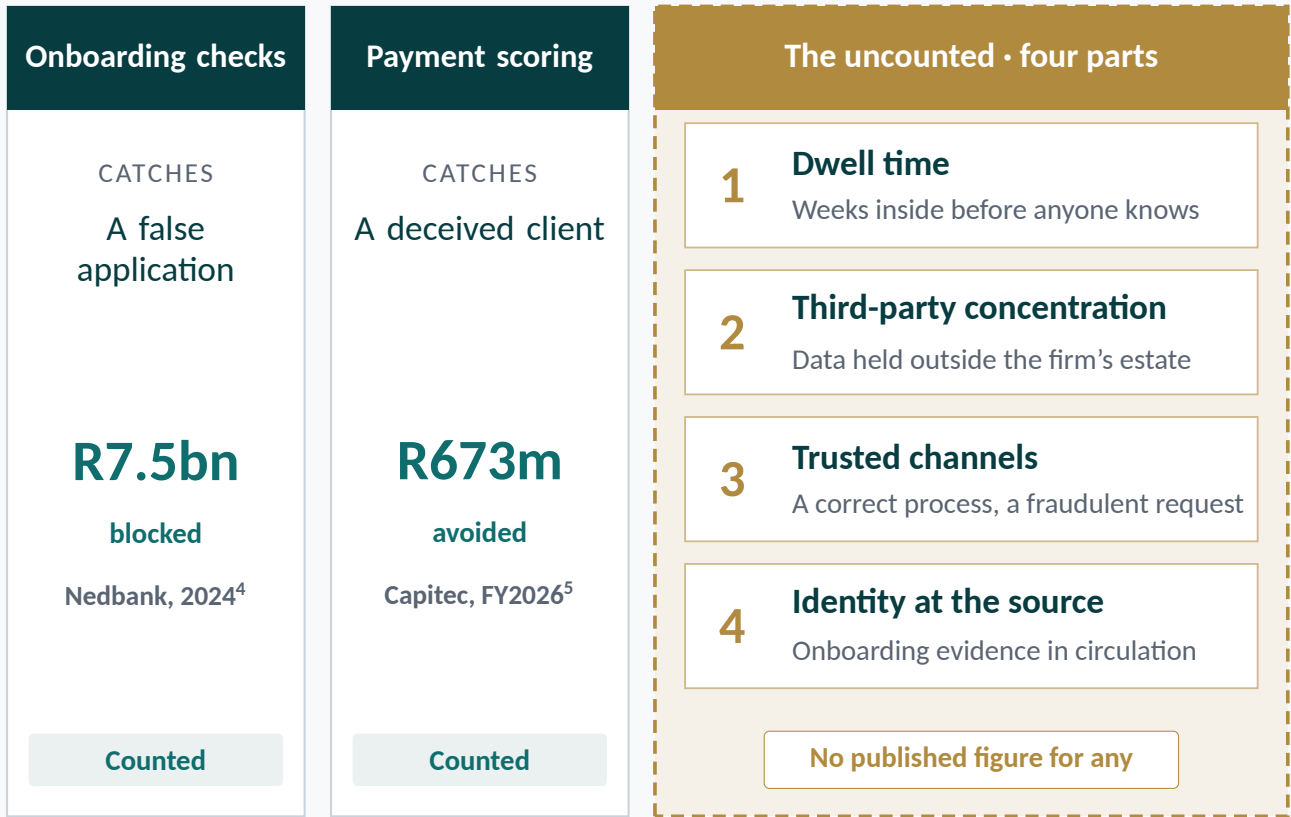


Protection for identity data therefore has to be judged against the lifetime of the person, not of the system, wherever the data travels. France's ANSSI has said it will stop certifying security products without post-quantum cryptography from 2027.³

Questions worth asking this quarter

- 1 How much identity evidence do we retain, for how long, and in how many environments, including those of our providers?
- 2 If identity documents for a portion of our clients were circulating today, how would our onboarding controls, and our reporting of them, reflect that?
- 3 What do we observe about accounts and access rights after they have been granted, rather than only at the point of granting them?
- 4 Is identity data protected, at rest and in transit, to a standard that will still hold when today's encryption no longer does?

Four gaps, one pattern



In each case every measured control performed as designed, no payment marked the moment of exposure, and no prevented-loss figure could capture it. The absence of a number has been read as the absence of a problem; these four cases suggest the problem has simply been sitting where nobody was counting.

Protecting what the counted controls cannot see

Kolm Shield is a Cape Town-based deep-technology cybersecurity company. Its proprietary, patent-pending quantum-safe architecture secures data at rest and in transit, including the identity records that cannot be reissued once exposed, and is designed to defend against the misuse of access that existing controls approve.

Sources: (1) Moneyweb, TimesLIVE and MyBroadband, September 2026, on the RelyComply-related notices, including EasyEquities' confirmation of 16 September that client data held by the provider was impacted. (2) The Register, 14 September 2026, including Revolut's statement; exposed-data details from customer notifications as reported. (3) Reuters, reporting remarks by ANSSI's chief of staff at France Quantum 2026, 16 June 2026. (4) Nedbank, as presented at the SAFPS International Fraud Summit, 2025. (5) Capitec Group, results for the year ended February 2026. Threat-actor statements throughout the series are reported as claims.

www.kolmshield.com