

The Dashboard Blind Spot

Why systems designed to protect vulnerable customers only see the people who ask for help

By Becky Hirst and Karen Cocks

The Hypothesis

When an institution moves a service onto a digital channel and then reports a high completion or adoption rate, that figure describes only the population that made it all the way through the process. It cannot describe the population that started the same process, met a barrier partway through, and left before anything was ever recorded. The working hypothesis behind this paper is that institutional protections for vulnerable customers activate almost entirely on disclosure rather than detection: something only becomes visible to the system once a person names their own struggle out loud. A customer who becomes frustrated and gives up without telling anyone has, by definition, disclosed nothing, and so remains invisible to every safeguard meant to catch them.

If that hypothesis holds, a bank, an airline, a hospital, or a government department can report near-universal success while a real and identifiable group of people experiences complete failure, and no dashboard anywhere in the organisation will show it. A 99% adoption rate and a 25% exclusion rate can both be true of the same institution at the same time, because they measure two entirely different populations. This paper tests that hypothesis against banking regulation and a recent public incident, then asks what changes once an institution accepts that its own success metric was never designed to see the people it fails.

Executive Summary

This paper examines a specific and repeatable failure inside institutions that have moved a service onto a digital channel: the measurement that proves success can also make an entire category of failure invisible. Independent research puts the population living with meaningful digital exclusion in Australia at close to a quarter of the country¹, rising to well over half among people over 75 and considerably higher again in the lowest-income households². Detailed reading of the Banking Code of Practice, ASIC's design and distribution obligations, and APRA's operational risk standard finds the same design choice repeated:

¹Australian Digital Inclusion Alliance, A National Approach to Digital Inclusion, 2025, https://www.digitalinclusion.org.au/wp-content/uploads/2025/06/2025_ADIA-A-National-Approach-to-Digital-Inclusion.pdf

²2025 Australian Digital Inclusion Index, https://digitalinclusionindex.org.au/wp-content/uploads/2025/10/ADII-Report-2025_V6-Remediated.pdf

protections for a vulnerable customer switch on only once that customer discloses their own circumstances, and the Code says so in its own words³. A live public incident in August 2026, in which a disability advocate was removed from a Virgin Australia flight after staff misclassified his wheelchair's power-assist motor, shows the identical mechanism working outside a screen, inside a single rigid rule applied by a frontline staff member with no authority to question it⁴. Read together, the regulatory record and the public incident point in one direction: institutions have built highly accurate instruments for measuring who succeeds, and no instrument at all for measuring who they lost along the way.

The Body: Research and Evidence

The Mechanics of a Blind Spot

The mechanism at the centre of this paper is straightforward once it is named. A dashboard that reports adoption, completion, or satisfaction is built from records of finished interactions, and every one of those records requires the customer to have reached the end of the process, whether that end point is a completed application, a logged transaction, or a survey filled out afterward. A customer who opens a form, struggles with an identity check, and closes the browser in frustration leaves behind no ticket, no flag, and no line item, because the system was never designed to log an ending that looks like failure. The result is a number that can be entirely accurate and still describe only part of the population an institution actually serves.

Set against that measurement gap, Australian data on basic digital access looks close to universal: 99% of Australians had home internet access and 99.7% used a device to go online in the six months to mid-2025⁵. Owning a device and a connection answers a different question entirely from completing a specific institutional process without giving up partway through. The distance between those two facts, having access and actually getting through, is exactly the space no dashboard in this research was found to measure.

The Self-Disclosure Trap in Banking Regulation

A close reading of the Banking Code of Practice, ASIC's regulatory guidance, and APRA's prudential standards surfaces a specific and repeated design choice behind this gap. Clause 52 of the Banking Code lists the circumstances that can heighten a customer's vulnerability, including age, disability, cognitive impairment, language barriers, and financial abuse, then

³Banking Code of Practice 2025, https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

⁴ABC News, 18 August 2026, <https://www.abc.net.au/news/2026-08-18/shane-hryhorec-disability-advocate-removed-from-virgin-flight/107049174>

⁵ACMA, How We Use the Internet, 2026, <https://www.acma.gov.au/sites/default/files/2026-02/How%20we%20use%20the%20internet%20-%20Executive%20summary%20and%20key%20findings.pdf>

states plainly that customers are encouraged to tell their bank about their circumstances, because otherwise the bank may not find out⁶. That single sentence hands the job of detection to the customer. The clauses covering First Nations customers, identifying suitable access arrangements, and low-income customers all follow the same structure: none of them activate until the person names their own circumstance first⁷.

One part of the Code breaks that pattern, which matters because it proves the alternative was always available to the people who wrote it. Two clauses require banks to employ a range of practices that can identify common indicators of financial difficulty and to proactively contact affected customers, genuine detection built from the bank's own data rather than a wait for disclosure⁸. That obligation was never extended to cover digital-channel struggle, failed identity verification, or onboarding abandonment, even though the drafting technique to do so already exists inside the same document.

ASIC's design and distribution obligations regime comes closest to a formal monitoring requirement over digital journeys. Regulatory Guide 274 requires issuers to keep reviewing whether a product's target market determination still holds, drawing on data that includes conversion rates and web analytics such as click paths⁹. The purpose of that review is product suitability, not exclusion detection, and there is no obligation to report drop-off data unless it also amounts to a significant dealing outside the target market¹⁰. APRA's operational risk standard, CPS 230, treats customer enquiries as a critical operation requiring a defined outage tolerance, a rule about system downtime rather than about one person failing a biometric check and giving up¹¹.

The industry's own compliance watchdog has already documented the resulting gap. The Banking Code Compliance Committee's 2021 inquiry into Part 4 of the Code found that compliance monitoring for online channels was markedly less mature than for contact centres, that only one bank in its review had built formal digital accessibility indicators such as screen-reader compatibility and colour contrast, and that even those indicators stopped short of measuring abandonment, completion, or drop-off rates¹². A follow-up inquiry

⁶Banking Code of Practice 2025, clause 52,

https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

⁷Banking Code of Practice 2025, clauses 48 to 57,

https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

⁸Banking Code of Practice 2025, clauses 173 to 174,

https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

⁹ASIC RG 274, September 2024, <https://download.asic.gov.au/media/etgm1amc/rg274-published-10-september-2024.pdf>

¹⁰ASIC, significant dealing notification requirements, <https://www.asic.gov.au/regulatory-resources/financial-services/design-and-distribution-obligations-significant-dealing-notification-requirements>

¹¹APRA, CPS 230, <https://www.apra.gov.au/standards/cps-230>

¹²BCCC, Part 4 inquiry report, December 2021, <https://bankingcode.org.au/app/uploads/2021/12/Banks-compliance-with-Part-4-of-the-Banking-Code-inclusivity-accessibility-and-vulnerability.pdf>

opened in January 2024 is examining financial abuse, interpreter access, and third-party authority, again without naming digital-journey abandonment as a metric in its own right¹³.

The consequence of these findings together is a governance model built entirely around people who are already customers. Vulnerability provisions apply once a bank is providing a service to a customer, which means a prospective customer who abandons onboarding before that relationship exists sits outside the framework altogether¹⁴. An institution can report accurate, even admirable, satisfaction and hardship-support figures for its existing customers while holding no visibility at all into the people who tried to become customers and could not.

The Same Pattern Outside a Screen

Everything examined so far in this paper happens on a screen: a banking app, an online form, an identity check completed at a keyboard. If the failure were really about screens, the fix would simply be a better website. But the hypothesis this paper is testing is narrower than that. It says the failure comes from a rule applied literally by whoever is closest to it, with no one authorised to notice when that rule does not work for the person in front of them, and no dashboard built to record it when it fails. If that is the real mechanism, it should not need a screen at all. In mid-August 2026, it did not.

Adelaide-based disability advocate Shane Hryhorec, who lives with C5 incomplete quadriplegia, was removed from a Virgin Australia flight from Sydney to Adelaide after staff applied a new rule requiring the power-assist motor on his wheelchair to be stored under his seat, a physical impossibility in his row given the business-class armrest in front of him and the placement of his service dog¹⁵. He had flown the same route without incident three times the preceding week, with the motor stored in the overhead locker each time. A staff member told him the earlier crews had done the wrong thing to accommodate him, converting a working arrangement into a violation on the spot¹⁶. Virgin Australia later explained that the device had been assessed primarily as a lithium battery rather than as a battery-powered mobility aid before boarding, so the relevant provisions were never applied¹⁷. A classification error inside the airline's own compliance process was resolved by removing the passenger, because no one on the aircraft had the authority to recognise that the rule itself, applied as written, made compliance impossible for the person in front of them. Virgin Australia

¹³BCCC, follow-up inquiry, <https://bankingcode.org.au/current-inquiries/inclusivity-accessibility-and-vulnerability-follow-up-inquiry/>

¹⁴Banking Code of Practice 2025, clause 54,

https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

¹⁵ABC News, 18 August 2026, <https://www.abc.net.au/news/2026-08-18/shane-hryhorec-disability-advocate-removed-from-virgin-flight/107049174>

¹⁶The Guardian, 19 August 2026, <https://www.theguardian.com/business/2026/aug/19/virgin-australia-apologises-to-disability-advocate-removed-from-flight-over-wheelchair-motor-ntwnfb>

¹⁷ABC News, 18 August 2026, <https://www.abc.net.au/news/2026-08-18/shane-hryhorec-disability-advocate-removed-from-virgin-flight/107049174>

apologised two days later and admitted it did not meet its own standards¹⁸. The airline's on-time performance and dangerous-goods compliance figures for that day almost certainly registered nothing unusual at all.

A rule that fails online and a rule that fails in front of two hundred passengers are the same design problem. They just run on different channels. Whatever fixes one has to fix the other, which is why the three questions this paper ends on apply to a process or a rule, never just to a website.

The Data

Independent measurement consistently finds a far larger excluded population than any institution's own adoption figures would suggest. The Australian Digital Inclusion Alliance's 2025 report states that close to 24% of Australians, more than 6.6 million people, remain either excluded or highly excluded from digital participation, and that among people with disability, 73% do not feel comfortable keeping up with technology change¹⁹. The 2025 Australian Digital Inclusion Index measured total exclusion separately at 20.6% nationally, climbing to 66.5% among people aged 75 and over and 63% in the lowest-income households²⁰.

On the regulatory side, the Banking Code Compliance Committee's own 2021 inquiry found that digital-channel compliance monitoring was markedly less mature than staff-mediated channels, and that no bank in its review was measuring abandonment or drop-off rates at all²¹. Every one of these figures comes from an external body measuring what the industry's own reporting leaves out, not from any bank's internal dashboard.

International experience shows that adding a person back into the process does not automatically close this gap. The United Kingdom's shared banking hubs, staffed by rotating bank employees to replace closed branches, were put forward as the face-to-face fix for digital-only banking. Lloyds Bank's own description of its community bankers states that for anything beyond a short list of simple tasks, staff will guide the customer through using their own device, which means the underlying digital process still has to work for the person to be served²². A parish treasurer's experience in August 2026 showed exactly what happens when

¹⁸The Guardian, 19 August 2026, <https://www.theguardian.com/business/2026/aug/19/virgin-australia-apologises-to-disability-advocate-removed-from-flight-over-wheelchair-motor-ntwnfb>

¹⁹Australian Digital Inclusion Alliance, A National Approach to Digital Inclusion, 2025, https://www.digitalinclusion.org.au/wp-content/uploads/2025/06/2025_ADIA-A-National-Approach-to-Digital-Inclusion.pdf

²⁰2025 Australian Digital Inclusion Index, https://digitalinclusionindex.org.au/wp-content/uploads/2025/10/ADII-Report-2025_V6-Remediated.pdf

²¹BCCC, Part 4 inquiry report, December 2021, <https://bankingcode.org.au/app/uploads/2021/12/Banks-compliance-with-Part-4-of-the-Banking-Code-inclusivity-accessibility-and-vulnerability.pdf>

²²Lloyds Bank, Community Bankers, <https://www.lloydsbank.com/help-guidance/everyday-banking/banking-near-you/community-bankers.html>

it does not: a fault inside Lloyds' own system stopped her from opening a new business account online after the old one was closed, and, by her account, branch staff standing in front of her had no manual way around the same fault²³. Putting a person at a counter changes who a struggling customer can talk to. It doesn't change whether the system behind that counter actually works.

The Gap

The people who disappear from a process rarely file a complaint. Most stop long before that point: a customer who abandons an online application rather than call a number that will ask them to explain something painful out loud, a person managing cognitive fatigue who closes a banking app halfway through identity verification and never opens it again, a carer handling someone else's affairs who cannot get through a process designed for a single, self-advocating account holder. The Banking Code's language of vulnerability assumes disclosure: a customer flags a hardship, a disability, or a language barrier, and the bank responds. It has no mechanism for the customer who never flags anything, because flagging itself is often the hardest part of the process for exactly the people the safeguard is meant to reach. Safety-net language only protects the person who knows to ask for it.

The same gap survives even a genuine attempt at a physical fix. A banking hub with a person behind the counter still routes the customer back onto their own phone for most of what they actually came in to do, so a customer who could not manage the digital process alone in the first place gains a friendlier setting to fail in, not a different outcome. The building changes. What the customer has to manage alone on their phone doesn't.

Conclusion: Testing the Hypothesis

The hypothesis this paper set out to test was that institutional protections for vulnerable customers switch on almost entirely by disclosure, leaving anyone who struggles without saying so outside the system's field of view. Every piece of evidence gathered here points the same direction. The Banking Code says as much in its own clauses. The regulator's own compliance watchdog found no bank measuring abandonment. A disability advocate was removed from a flight because no one in the chain had the authority to say a rule had failed, not the passenger. Different institutions, solving different problems, kept arriving at the same design choice and the same blind spot.

The point of view this research supports is a direct one. An institution's success metric and its safeguard for vulnerable customers cannot be built from the same population without leaving someone out. Measuring who completed a journey will always undercount who

²³The Guardian (Anna Tims, "Lloyds Bank is holding on to our urgently needed £5,500"), 25 August 2026, <https://www.aol.co.uk/articles/lloyds-bank-holding-urgently-needed-060050000.html>

needed help along the way, because the two groups are only visible through completely different instruments, and most institutions have only built one of them. A bank, an airline, a hospital, or a government department that wants an honest picture of who its process is failing has to go looking for the people who are missing from its data, deliberately, before it can claim to know what its own dashboard is actually measuring.

That means treating the people who disappear from a process as a measurable population with a cost that gets reported and acted on, the same way an institution already treats the customers who succeed. What is the dashboard costing the people who need this service and cannot get through it? Until that question has an answer, a 99% success rate doesn't measure how well the system works. It measures how early someone had to be excluded to disappear from the count.

The Fix: The EVA Method

The evidence in this paper points to the same fix wherever it was tested, in banking regulation, in ASIC's own data capability, and in the Virgin Australia incident. Each shows a working part of it already sitting inside the institutions examined, just never used for this purpose. Building it out means three things: engage, validate, adapt.

Engage

An institution that wants to see who its process has failed has to go looking for them, rather than wait for them to surface in an existing customer channel. That means engaging directly with the people who already sit outside the system, community organisations, disability advocates, aged-care services, financial counsellors, rather than treating the customer-service queue as the only source of signal. Regulatory Guide 274 already requires ASIC-regulated issuers to hold click-path and conversion data capable of supporting exactly this kind of outreach²⁴; nothing currently requires that data to be pointed at the missing population rather than at target-market review.

Validate

Clauses 173 to 174 of the Banking Code already require banks to detect a problem rather than wait to be told about it²⁵, and that same obligation needs to extend past financial hardship into digital-channel struggle, failed verification, and onboarding abandonment. In practice, that means training frontline staff to treat a person's own account of their situation as sufficient grounds to act, not something that must be proven first. That is the specific gap

²⁴ASIC RG 274, September 2024, <https://download.asic.gov.au/media/etgm1amc/rg274-published-10-september-2024.pdf>

²⁵Banking Code of Practice 2025, clauses 173 to 174, https://www.ausbanking.org.au/wp-content/uploads/2024/06/Banking-Code-of-Practice_2025.pdf

the Hryhorec case exposes: no one in the chain had the authority to accept, on his word, that the rule as written could not be followed.

Adapt

The mechanism itself has to change, not only the monitoring around it. That means building abandonment and drop-off tracking into the dashboard alongside completion and adoption, so the population that leaves a process becomes as visible as the population that finishes it, and building a genuine non-digital route back into the process for the person the digital one failed, rather than another prompt to retry the same path that already defeated them.

Every part of this method already has a precedent inside the evidence this paper reviewed. The capability exists in each institution examined. What has not yet happened is a decision to point that capability at the population no dashboard was ever built to count.

FTS WHITE PAPER

Version log

The Dashboard Blind Spot, by Becky Hirst and Karen Cocks

Our white papers are forever evolving. As our thinking deepens and the research grows, we update them. This log shows the date of the latest version of this paper and the changes made along the way.

VERSION	DATE	WHAT CHANGED
1.1	13 September 2026	Background updated to the warm ivory of the series, and this version log added.
1.0	31 August 2026	Original publication.