



ARMIDALE

PERSPECTIVE

Nobody Answers Any More

The largest cost of scams is carried by people who were never scammed.

Leslie Falvey · September 2026

Every official record of fraud is built on one measure: the money taken from victims. It is the figure governments publish, the figure the industry argues about, and the figure every reform is judged against.

It leaves out the larger cost. Consider the person who lets an unknown number go to voicemail, ignores a text message, abandons a purchase from a shop they have not used before, or deletes a genuine alert from their bank because it looks like the last one that was fake. None of them has lost a penny. Each is behaving sensibly. Together they impose a cost on every legitimate business that needs to reach a customer, and the scammer pays none of it.

The retreat, and who is making it

Armidale's 2026 consumer survey for the GSMA asked about it in Southeast Asia. Forty-one per cent of consumers have changed or limited their contact details,

which includes ignoring unknown calls and links. Nineteen per cent will re-engage only through a number they have dialled themselves. Counting those alongside consumers who have cut back on online transactions, 56% avoid inbound contact or transactions because of scam concerns.

The important finding is who is doing it. Among consumers who have never been scammed, the numbers match the full population to within a point at every step. This is not victims flinching after the event. It is the general population adjusting to what it believes the environment is.

It also tracks what people can recognise. Among consumers who could identify one artificial intelligence technique in the scams they had seen, 28% had changed or limited their contact details. Among those who could identify five or more, 58% had.

The people withdrawing are not the people who lost money. They are the people who worked out what was coming.

The pattern holds outside the region.

- Belgium: a victimisation study of around a thousand people, cited in the standard academic survey of what cybercrime costs, found 16.5% of the population reducing or stopping certain online activities as a security measure, including 10.4% for online shopping and 5.9% for electronic banking. Its authors call that the best evidence available for the chilling effect, which is a fair description of how little there is
- Six Western markets: Hiya, which sells spam protection to mobile operators and therefore has an interest in the answer, surveyed more than 12,000 consumers across the United States, Canada, the United Kingdom, Spain, France and Germany. Only 14% answer a call from a number they do not recognise, and 34% say their trust in phone calls has fallen in the past year, against 16% saying it has risen

Where the harm goes when a channel empties

Australia publishes enough to follow what happens next. Australian telecommunications providers blocked over 492.7 million scam calls and over 153.5 million scam text messages during 2025, in a country of about 27 million people. Reports to Scamwatch, the national scam reporting service, with the contact method recorded as a phone call are now 73.7% below their 2021 level.

- Phone: withdrawal worked. Losses fell 32% in 2025, from A\$107.2 million to A\$72.5 million, the largest fall of any contact method. But the people who still answer lose far more each. The median loss on a phone report is A\$3,800, against A\$400 across all Scamwatch reports
- Text message: the opposite. Reports fell 62.4% in a single year, from 77,365 to 29,058, while losses on that channel rose from A\$14.0 million to A\$17.9 million. Fewer people reached, and more lost by the ones who were
- Online contact: losses rose 21.8% in 2025 to A\$158.5 million, and reports carrying a loss rose 31.8%

Withdrawal is effective for the person who withdraws. It redistributes the harm rather than removing it, onto whoever still answers and onto the channels that cannot be screened.

Why none of it is counted

A cost gets counted when it lands on someone who has to book it. Every part of this one lands on somebody who did not cause it and cannot invoice for it.

- The bank that cannot reach a customer to verify a payment absorbs the cost of a second attempt
- The health service whose patient will not take a call from an unfamiliar number absorbs the missed appointment
- The retailer nobody has heard of absorbs the abandoned basket
- The operator carries a network that people trust less each year

None of them can point to the transaction that did not happen, and none of them can attribute it to a scam.

The frameworks for valuing this are not missing. One established method values a crime by what people would pay in advance to reduce their risk of it, which captures the behaviour of everyone who is frightened rather than only those who are robbed. The standard academic survey of cybercrime costs takes a different route, and carries a category that reaches part of the same ground, treating the inconvenience of legitimate messages caught by spam filters as a defence cost rather than a loss.

What is missing is a standing measure. Statistical agencies do ask adjacent questions, and European surveys have asked for years whether people avoid online shopping or banking over security concerns. What no government publishes is a continuing series of scam-driven avoidance, split by whether the person has ever been a victim, set beside the loss total it belongs with. Fraud gets counted the way it does because the money taken is easy to observe, not because it is the largest part of the harm.

The merchant side is worse. Published figures on how many legitimate orders get refused come almost entirely from vendors and industry surveys, and no official statistics series measures it. The absence is the finding.

Rational adaptation, and why it still costs

The strongest objection is that this is not a harm but an adjustment, and a cheap one.

Screening a call costs nothing. Substitutes are everywhere: the customer who ignores a text opens the app instead. People routinely trade a small inconvenience for a reduction in risk, and calling that a welfare loss sentimentalises a sensible precaution. The objection has authority behind it. The same academic survey that supplies the best withdrawal figures also warns that low take-up of a channel is not a reliable measure of fear, because take-up varies for many reasons that have

nothing to do with crime. And the strongest call-avoidance data comes from a company that sells the remedy.

All of that should be conceded. What survives it is the distribution. The people bearing the cost are not the people making the decision, and they are not the people who caused the risk. The scammer bears none of it. The response is rational for each person and expensive in aggregate, which is the textbook definition of a cost that will keep growing until someone is made to own it.

And it rises with sophistication. Contact withdrawal moving from 28% to 58% as people recognise more artificial intelligence in what reaches them is a forecast, not a snapshot. Withdrawal increases as the attacks get better, whether or not anyone loses money.

Count it, or keep reporting the wrong number

For governments, the fix is a survey question, not a programme. National crime and consumer surveys already reach the right samples. Add a standing measure of avoidance: the share of adults who have stopped or limited a channel, a payment type or a class of purchase because of scams, split by whether they have ever been a victim. Publish it beside the loss total, every year, on the same page.

That pairing matters more than either number alone. A falling loss total beside rising avoidance is not a programme working. It is a population solving the problem by leaving, and a government claiming the credit.

For industry, the measurement already exists inside the firms losing the most. Operators know their answer rates. Banks know how many customers they cannot reach on the first attempt. Retailers know how many baskets are abandoned at the payment step. Those are treated as marketing numbers. They are the closest thing anyone has to a running count of what scams cost people who were never scammed, and not one of them is published.

Sources and method

Armidale for the GSMA, ASEAN Consumer Scam Report 2026, for the withdrawal, re-engagement and artificial intelligence recognition figures. R. Anderson, C. Barton, R. Böhme, R. Clayton, C. Ganán, T. Grasso, M. Levi, T. Moore and S. Vasek, Measuring the Changing Cost of Cybercrime, Workshop on the Economics of Information Security, 2019, for the Belgian victimisation study (fieldwork by Paoli and colleagues for the Belgian Cost of Cybercrime project), the chilling-effect assessment, the defence-cost category and the warning about take-up as a measure of fear. National Anti-Scam Centre (Australia), Targeting Scams 2025, March 2026, for the blocked-call and blocked-message volumes, the contact-method report trends, the loss totals for phone, text message and online contact, and the median losses. Hiya, State of the Call 2026, a Censuswide survey of more than 12,000 consumers in the United States, Canada, the United Kingdom, Spain, France and Germany, published by a firm that sells spam protection to mobile operators.

The median loss of A\$3,800 is for Scamwatch reports with the contact method recorded as a phone call, and the A\$400 comparator is the median across all Scamwatch reports. Contact-method figures are Scamwatch only, not the combined national total, which draws on five reporting bodies. Blocked-call and blocked-message volumes are provider-reported activity, not avoided harm, and the totals they are drawn from are not published. No figure in this report has been rescaled, modelled or extrapolated.

About the author

Leslie Falvey is the founder of Armidale, a Singapore advisory firm, and author of the GSMA ASEAN Consumer Scam Report 2026, now in its third edition across six ASEAN markets and India. His work follows how consumers encounter, report and resolve scams, and treats fraud as an economic harm whose largest costs fall outside both the victim and the firm that failed to resolve the case.

About Armidale

Armidale is a Singapore advisory firm working at the intersection of payments, fraud and digital commerce, combining primary consumer research with strategy and execution for operators, financial institutions and industry bodies.

© 2026 Armidale Pte. Ltd. · Published September 2026 · armidale.co · Provided for information and does not constitute legal, financial or security advice.