



Secretariat: Second National Action Plan Consultation
Department of Social Services

31 July 2026

Dear Secretariat

Thank you for the opportunity to make a submission.

In 2019, as a bank executive, I discovered that customers were using payment descriptions to send threatening and abusive messages to their former partners. More than 8,000 people did it in a single three-month period. Before we looked, we had no idea. Once we looked, we could design it out.

That is the whole argument of this submission. Perpetrators of domestic and family violence use the products, services and systems Australians rely on every day as instruments of control. Those systems were designed for people in healthy relationships with equal access to money. When we design for the perpetrator instead, we prevent harm before it happens – and we do it at a scale no crisis service can reach.

The National Plan already commits business to designing products and services that are safe and prevent misuse, and to perpetrator accountability. The First National Action Plan did not deliver on that commitment. The Second National Action Plan must.

This submission makes five recommendations. It builds on, rather than repeats, my submission to the Parliamentary Joint Committee on Corporations and Financial Services and on my Designed to Disrupt® discussion papers.

I would welcome the opportunity to discuss this submission.

Yours sincerely

A black rectangular box redacting the signature of the sender.

A black rectangular box redacting the name of the sender.

Founder and Director, Flequity Ventures
Adjunct Associate Professor, UNSW School of Social Sciences



Submission

Designed for safety.

July 2026

Table of contents

Introduction.....	3
Recommendations.....	5
1. Finish what the national financial abuse inquiry started.....	5
2. Financial safety. By design.....	6
3. Perpetrator accountability.....	8
4. Count business in.....	9
5. Coordinate the response.....	10
Appendix.....	Error! Bookmark not defined.

About us.

Flequity Ventures is a social enterprise on a mission to disrupt financial abuse a gender bias through more flexible, safe and equitable product and service design. It's our contribution to closing the economic gap for women.

Our founder and Director, [REDACTED], created the financial safety by design framework in 2022. She has since facilitated its adoption across banks, insurers and essential service providers, and it is informing policy development and regulatory guidance in Australia. [REDACTED] is an Adjunct Associate Professor at UNSW School of Social Sciences, an adviser to the World Bank's International Finance Corporation, and a recognised expert advising the Commonwealth government and Bank of Papua New Guinea. She is also founder of the Financial Safety Alliance and co-founder of the One Generation business alliance against domestic and family violence.

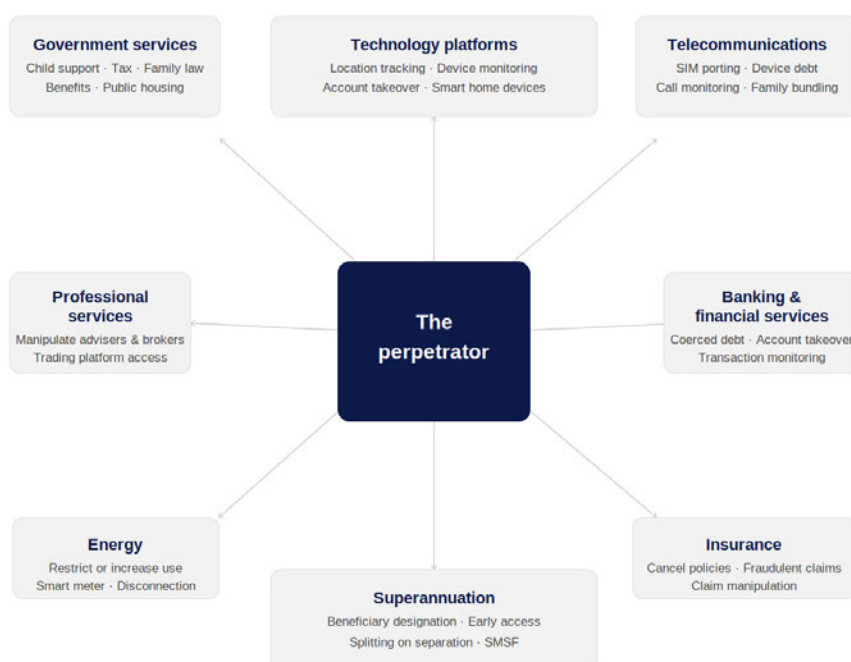
Introduction.

Safety isn't accidental. It's designed.

As Australia's next five-year plan to end gender-based violence is being developed, one of the most significant, impactful opportunities to prevent harm, preventing financial abuse, is at risk of being overlooked.

Financial abuse involves the use of money to gain power and control over a partner or family member, limiting their independence. It is a far-reaching form of domestic and family violence, with 1.6 million women directly affected in their lifetime¹ and costing victim-survivors an estimated \$5.7 billion per year.²

Perpetrators weaponise financial products, services and systems to maintain control and prevent victim-survivors from accessing the resources they need to escape, find safety and ultimately, start a new life. The economic impact is stark, with women who have been financially abused less likely to be in employment and nearly four times more likely to rely on government payments as their main source of income.³ The abuse can also take a profound emotional, social and mental toll at a time of acute vulnerability (see appendix).



While perpetrators have become sophisticated users of financial products, legal systems, digital platforms and government infrastructure as weapons of control, our national public conversation remains largely focused on refuges, counsellors and policing. That's like trying to address road trauma by only funding hospitals.

The most effective way to combat financial abuse is to prevent it. Importantly, preventing and disrupting financial abuse is possible, with progress being made through reforms to the tax and social security systems at the federal level, and to the rental bond system in New South Wales. Business is also stepping up with more than 80 brands

¹ Summers, A, Shortridge, T, and Sobeck, K, [The Cost of domestic violence to women's employment and education](#), University of Technology Sydney, 2025.

² The cost of financial abuse in Australia, Deloitte Access Economics for Commonwealth Bank of Australia, 2022.

³ Summers, A, Shortridge, T, and Sobeck, K, [The Cost of domestic violence to women's employment and education](#), University of Technology Sydney, 2025.

across a range of sectors acting to change their policies, terms and conditions to ban the misuse of their products for financial abuse.

While this progress is welcome, it is slow, lacking coordination and far from complete. More must be done. Urgently.

Australians' financial lives are lived online. Digital identity, money, services and communication are all available – and exploitable – at the click of a button.

This already makes financial abuse almost effortless and artificial intelligence is now accelerating this. AI can make deception more convincing, fabricate documents and evidence at speed, and impersonate financial professionals or the victim-survivor themselves. Every month the tools get better. Without targeted and coordinated intervention across sectors, financial abuse becomes cheaper, faster and harder still to escape.

Financial abuse is both a gender-based violence issue and an economic security issue. It sits between the National Plan and the Government's women's economic equality agenda⁴ – and because it belongs to both, it is currently owned by neither and the response is fragmented. Which leaves victim-survivors navigating multiple systems and suffering the economic impacts, while perpetrators exploit and manipulate systems that have not been built with them in mind.

If we're serious about prevention, reducing coercive control and designing safer systems, then safety by design must become part of Australia's prevention architecture and combatting financial abuse must be prioritised through dedicated action under the Second National Action Plan.

This submission complements our Designed to Disrupt® reports and submission to the financial abuse inquiry in 2024. It makes five recommendations:

1. Finish what the national financial abuse inquiry started.
2. Financial safety. By design.
3. Count business in.
4. Coordinate the response.
5. Perpetrator accountability.

The National Plan already made this commitment. The Second National Action Plan is the opportunity to keep it.

⁴ Working for Women: A Strategy for Gender Equality, Commonwealth of Australia, 2024; Women's Economic Equality: A 10 year plan to unleash the full capacity and contribution of women to the Australian economy, Commonwealth of Australia, 2023.

Recommendations.

1. Finish what the national financial abuse inquiry started.

The consultation paper identifies systems abuse as a priority and asks how to address it across sectors. But financial abuse is currently treated as a symptom of domestic and family violence rather than one of its primary tactics and one of its most enduring harms. It is largely absent from the paper, and it was largely absent from the First National Action Plan.

We have a roadmap. The Parliamentary Joint Committee on Corporations and Financial Services delivered it in December 2024: 61 recommendations, adopted unanimously, endorsing safety by design as the strategy for preventing financial abuse in the finance sector.⁵

The Government is acting on parts of it. The 2026-27 Budget provided \$182.6 million to reform the child support system, and Treasury has consulted on coerced directorships and on preventing perpetrators from accessing their victim's superannuation death benefits. But more than 18 months on, there has been no official response to the report as a whole.

Industry has also moved, with education, awareness and new guidance. But there is more to do – 10 of the inquiry's recommendations could be introduced by the private sector without government reform, yet there has been incremental progress.

Recommendation 1

Prioritise the prevention of financial abuse.

- a. Include a dedicated action on preventing financial abuse in the Second Action Plan, recognising it as both a form of gender-based violence and a driver of women's long-term economic insecurity.
- b. Incorporate the recommendations of the financial abuse inquiry which relate to prevention into the Second National Action Plan, so they have an owner, timeframe and measure.
- c. Align the Second Action Plan with the Government's women's economic equality agenda, so that financial abuse is addressed as an economic security issue as well as a safety issue.

⁵ Financial abuse: an insidious form of domestic violence, Parliamentary Joint Committee on Corporations and Financial Services, December 2024

2. Financial safety. By design.

Seven separate reviews have now examined how systems are weaponised for abuse, but each looked at only a slice. Most recommended safety by design as an approach to disrupt the harm:

- The Parliamentary Joint Committee examined the finance sector and made 61 unanimous recommendations.⁶
- The Rapid Review examined government systems and prevention.⁷
- The Essential Services Commission Victoria examined energy and water, commissioning Flequity to develop a Designed to Disrupt® report as part of its safety by design initiative.⁸
- The eSafety Commissioner and the proposed Digital Duty of Care cover online services and a defined list of harms.⁹
- The South Australian Royal Commission examined one State's systems and services and made 136 recommendations.
- The Commonwealth Ombudsman examined the Child Support System.
- The Tax Ombudsman examined the tax system.

Separately, since 2022 Flequity has examined four sectors – banking, general insurance, utilities, telecommunications (yet-to-be published) as part of its Designed to Disrupt® series, in addition to reviewing whether and how NSW Government products and services may be at risk of being weaponised.¹⁰

None of these reviews have looked at the whole picture.

Yet perpetrators move between sectors, exploiting the products, services and system we use every day with technology increasing the speed and scale of harm.

Change the Story addresses the drivers of violence: the attitudes, norms and power structures that make perpetration more likely.¹¹ Until Australia achieves those strides in gender equality, we need to redesign the systems misused for abuse.

Instead safer design is being introduced one sector at a time, under different names, with different levels of force.

The proposed Digital Duty of Care will legislate safety by design for online services and a defined list of harms.¹² Financial abuse and coercive control are absent from that list. The ACMA's telecommunications domestic, family and sexual violence standard watered down safety by design language and replaced it with "inclusive design", following a public consultation period on the draft.¹³ Essential services regulators use it in guidance.¹⁴ Finance uses it voluntarily.¹⁵

The Australian Government has recognised the weaponisation of its services and systems. Following National Cabinet in September 2024 it began an audit of Commonwealth systems to identify where they are being weaponised, overseen by a Secretaries Working Group on Gender-Based Violence and supported by the Office for Women in the Department of the Prime Minister and Cabinet. The Office for Women has since published

⁶ Financial abuse: an insidious form of domestic violence, Parliamentary Joint Committee on Corporations and Financial Services, December 2024.

⁷ Unlocking the Prevention Potential: accelerating action to end domestic, family and sexual violence, Rapid Review Expert Panel, August 2024.

⁸ Essential Services Commission Victoria safety by design partnership; Better practice in responding to family violence, Essential Services Commission, 2022.

⁹ A Digital Duty of Care for Australia, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, May 2026.

¹⁰ Rapid review of prevention approaches: Australian Government, state and territory collective response – 28 November 2025, Department of the Prime Minister and Cabinet

¹¹ Change the story, Our Watch

¹² A Digital Duty of Care for Australia – Developing a duty of care framework for online services used by Australians, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, May 2026

¹³ Telecommunications (Domestic, Family and Sexual Violence Consumer Protections) Industry Standard 2025, Australian Communications and Media Authority, registered 11 June 2025.

¹⁴ Safety by Design Partnership, Essential Services Commission Victoria, May 2025; A safer energy market for customers affected by family violence, Australian Energy Regulator, May 2025.

¹⁵ Keeping banking customers safe from financial abuse, Australian Banking Association, 1 November 2024; Best Practice Guidance: Family and Domestic Violence Policies, Council of Australian Life Insurers, February 2025.

guidance for agencies on embedding safety by design in government systems, built on three principles and a five-phase approach that begins with understanding how systems are misused.

This is the most advanced application of safety by design in the country. It is also expressly not prescriptive, it binds no one, and it reaches Commonwealth agencies alone. States and territories administer housing, child protection, courts, policing, utilities and rental bonds – systems perpetrators use constantly. Business is outside it altogether.

There is an opportunity to harmonise the approach and Australia has done this before. The National Principles to Address Coercive Control gave Commonwealth, State and Territory governments a shared definition and a shared standard without requiring identical legislation.¹⁶

Recommendation 2

Make safety by design part of Australia's prevention architecture.

- a. Name safety by design in the Second National Action Plan as a national prevention approach, applying to domestic, family and financial abuse – not only to online and child safety harms.
- b. Develop national principles for safety by design, agreed by all jurisdictions, modelled on the National Principles to Address Coercive Control.
- c. Commit to Including technology-facilitated financial abuse and coercive control as harms in scope of the Digital Duty of Care, while the legislation is being drafted.
- d. Extend the Australian Government's audit of Commonwealth systems to the states and territories through National Cabinet, which commissioned that audit in September 2024, so every jurisdiction reviews the systems perpetrators exploit, remediates the harm and applies safety by design to their redesign.
- e. Implement knowledge-sharing protocols between jurisdictions to drive consistency and ensure better practice is adopted nationally.

¹⁶ National Principles to Address Coercive Control in Family and Domestic Violence, Attorney-General's Department, 2023.

3. Perpetrator accountability.

Perpetrators do not think in sectors. They think in opportunities — for power and for control. They will use a smart lock to trap a partner at home, a telco account to track her, a credit card to saddle her with debt, an insurance cancellation to punish her, a tax return to manufacture a debt in her name.

Behaviour change programs reach hundreds of men at a time and matter deeply. But business reaches millions, and it sees perpetration in real time, in data, before police or frontline services ever do.

We know this works, because it has already been done. After Australian banks began detecting abusive messages in payment descriptions, they blocked more than one million messages in real time from more than 300,000 customers and sent warning letters to thousands. More than 90 per cent of those who received a letter stopped.¹⁷

We did not change the technology. We changed the expectation.

Those same detection systems now feed law enforcement. AUSTRAC created a suspicious matter reporting category for abusive text and emojis used in criminal communication.¹⁸

No funded prevention program in this country can show reach and cessation at that scale, for that cost.

This is not a new idea for the National Plan. The First Action Plan already commits to strengthening systems to better hold perpetrators accountable. The Second Action Plan should carry that action forward and widen it beyond government systems to the commercial products and services perpetrators use every day.

Recommendation 3

Use business systems to disrupt perpetrators.

- a. Recognise detection and disruption of abuse within commercial products and services as a prevention and early intervention measure under the Second Action Plan.
- b. Support all sectors to adopt terms and conditions specifying domestic and financial abuse as unacceptable customer behaviour, and to communicate the consequences of misuse.
- c. Acknowledge that the tactics and impacts of financial abuse are consistent with fraud, scams and theft, and move to treat it as a financial crime.
- d. Establish intelligence-sharing protocols between business, regulators and law enforcement to accelerate disruption.

¹⁷ Designed to Disrupt: Reimagining banking products for financial safety, Catherine Fitzpatrick for the Centre for Women's Economic Safety, 2022

¹⁸ Preventing misuse and criminal communication through payment text fields, Financial Crime Guide, AUSTRAC & Fintel Alliance, November 2021

4. Count business in

Perpetrators of financial abuse use a range of tactics, some of which are unintentionally enabled or exacerbated by the design of commercial products, services and systems. The products and platforms Australians rely on every day, like joint accounts, digital wallets, insurance policies and superannuation, were not designed to resist malicious misuse by a partner.

Wherever there is a joint account or online access, there is an opportunity for misuse. In the hands of abusers, these products and digital services become weapons of financial destruction, leaving victim-survivors with damaged credit scores, unmanageable debt and entrenched poverty.

Yet business is already part of the system. Women are more likely to talk to their bank about economic abuse than to contact a specialist domestic violence service. For financial abuse, business is frequently the first responder – and often the only organisation holding evidence of what is happening.

Safety by design also removes a barrier the rest of the system cannot. Product safeguards work whether or not a victim-survivor discloses, whether or not she has proof, and whether or not the person in front of her recognises what she is describing.

Business will not get there on its own. In January we reviewed more than 150 bank and general insurance brands to see how many had adopted the safety measures recommended by the inquiry. Fewer than a third had added a quick exit button to their website, the simplest safety feature there is. Only 13 per cent of banks offered multiple offset accounts to protect victim-survivors from having joint offsets cleaned out. Only 16 per cent of insurers had a conduct of others clause allowing claims to be paid that would otherwise be denied under a malicious damage exclusion.

Where business has moved, it has moved fast. More than 80 brands across 10 sectors have introduced terms and conditions specifying financial abuse as unacceptable customer behaviour, offering greater protection to more than 20 million customers. Our research shows 96 per cent of Australians want these protections. The question is no longer 'should we do this', it is 'why haven't we'?

Critically, the same threat assessment approach that cyber security and fraud teams apply instinctively, understanding the threat actors and their methods, has not yet been systematically applied to financial abuse. Flequity Ventures' Design like a domestic abuser™, an evidence-backed AI-assisted simulation, demonstrates this approach is both effective and powerful, allowing companies to see how their product features are being weaponised then work through the vulnerabilities and control across the whole customer journey.

The eSafety Commissioner's [Safety by Design](#) framework, and the positive duty model already applied to sexual harassment in workplaces, provide proven regulatory precedents for requiring protective action.

Business must be required to assess and remediate the risks of product weaponisation and Directors must bear responsibility for ensuring this happens. Safety must be proactively designed in.

Recommendation 4

Enhance business expectations for safety by design and duty of care

- a. Include business as a delivery partner in the Second National Action Plan, with measurement and reporting.
- b. Commit to developing a positive duty on business to prevent the misuse of their products, services and systems for domestic and financial abuse.
- c. Commit to clarifying that the risk of product weaponisation, which in the worst cases can lead to the death of a customer, is material and foreseeable and should be considered by directors as part of the duty of care and diligence.

5. Coordinate the response.

Prevention efforts are fragmented across sectors, regulators and jurisdictions, while perpetrators move freely across all of them. The only person who sees the whole picture is the victim-survivor.

We know how to fix this, because we have just done it for another crime using strikingly similar social engineering tactics to cause financial harm – scams.

The cost disparity between financial abuse and scam illustrates the inconsistency clearly: \$5.7 billion¹⁹ – the estimated direct annual cost of financial abuse to Australian victim-survivors is more than double the \$2.18 billion lost to scams in 2025.²⁰

Scam prevention efforts have resulted in a National Anti-Scam Centre, a legislated Scams Prevention Framework imposing obligations across banks, telcos and digital platforms, dedicated Commonwealth funding and a national public education campaign.²¹

There should be a similar response to financial abuse.

In July 2026 the Prime Minister made the same argument about a different challenge.

Because artificial intelligence reaches every minister and department, he said, the Government's response had until then been "issue-by-issue, sector by sector".²² His answer was to stop working that way: a coordinating office established inside the Department of Prime Minister and Cabinet, a single national framework in place of overlapping rules and agreement to be sought from Premiers and Chief Ministers at National Cabinet. He placed AI alongside civil aviation in the 1920s and genetics in the 1990s – technologies where Australia chose coordination over drift, and where the discipline fell on government as much as on industry.

Financial abuse reaches every Minister and Department too. Treasury, Social Services, the Attorney-General's portfolio, Communications, Services Australia, the Australian Taxation Office, and every State and Territory system a perpetrator can touch.

Our response has been issue-by-issue, sector by sector. The Government has just demonstrated what to do about that.

The Australian government has already built this machinery for its own systems, inside the Department of Prime Minister and Cabinet. The systems abuse audit stops at the edge of government – it does not reach the sectors perpetrators use every day.

Recommendation 5

Coordinate a national response to financial abuse.

- a. Acknowledge that the tactics and impact of financial abuse are consistent with other financial crimes such as fraud, scams and theft, and that artificial intelligence is empowering abusers with new and rapidly evolving tools.
- a. Establish a Financial Abuse Prevention Centre, modelled on the National Anti-Scam Centre and the Scams Prevention Framework, to coordinate cross-sector, public-private action to prevent financial abuse.
- b. Include financial abuse indicators in the outcomes and measurement framework for the Second National Action Plan.
- c. Review all government systems and services that hold information or make payments to assess whether services or systems could enable or exacerbate financial abuse.
- d. Implement knowledge-sharing protocols amongst jurisdictions and across sectors to drive consistency and ensure best-practice approaches are adopted nationally.

¹⁹ The cost of financial abuse in Australia, Deloitte Access Economics for Commonwealth Bank of Australia, 2022.

²⁰ Continued action critical to combat fraud as annual scam losses exceed \$2 billion, National Anti-Scam Centre, 2026.

²¹ Ibid.

²² The Hon Anthony Albanese MP, AI in Australia's interests, The University of Sydney, 15 July 2026.