



20 March 2023

Committee Secretary  
Electronic Transaction Act Consultation  
PO Box 6100  
Parliament House  
Canberra ACT 2600

By email: [eta@ag.gov.au](mailto:eta@ag.gov.au)

Dear Committee,

### **Submission into the Electronic Transaction Act Consultation in Australia**

Thank you for the opportunity to provide input to the consultation into the *Electronic Transactions Act 1999* (Cth) (ETA). Our input is narrowly focused on responses to economic abuse based on casework experience. We consent to this submission being made public.

### **Economic Abuse Reference Group**

The Economic Abuse Reference Group (EARG) is an informal group of community organisations which work collectively with government and industry to reduce the financial impact of family violence. Members include domestic and family violence (DFV) services, community legal services and financial counselling services, and we involve other organisations in our work where relevant.

This submission was prepared with input from contributors to the EARG. Some of our members have experience (as lawyers or financial counsellors) assisting clients who have experienced economic abuse. See more details about EARG [here](#).

### **Economic abuse and electronic transactions**

Economic abuse, also described as financial abuse, is a form of family, domestic and sexual violence. It has significant and devastating impacts at an individual, community and societal level. Economic abuse can take various forms, including accruing debt or other liabilities in the other person's name, not contributing to joint loans, controlling all finances, not making shared financial decisions, withholding necessities, preventing someone from obtaining or remaining in employment, and stopping someone from accessing education or a means to become financially independent. Economic abuse often occurs alongside other forms of abuse such as physical and emotional abuse, and sexual violence.

Financial abuse is a hidden epidemic in Australia. A recent report by Deloitte Access Economics found that 43 Australian women were subjected to financial abuse every hour in 2020.<sup>1</sup> Around 85% of women who access domestic and family violence (DFV) services in Australia say that they have experienced some level of financial abuse in their relationship.<sup>2</sup> A 2017 study into the prevalence of economic abuse between intimate partners found that 11.5% of Australians had experienced it and that women experience it at higher rates (15.7%) than men (7.1%) The true prevalence is likely far higher given the underreporting of domestic and family violence.<sup>3</sup> These gender differences are important because it is well understood that family, domestic and sexual violence is gendered, and that women are the majority of victims and experience more severe consequences.<sup>4</sup>

### How electronic transactions can facilitate economic abuse

Electronic transactions can be the means through which financial abuse is perpetrated, for example through perpetrators coercing victim survivors to sign loan documents electronically, or simply committing identity fraud. While physical signatures or wet ink signatures do not necessarily prevent this happening, they do add an extra layer of protection and screening to ensure that signatures are not obtained fraudulently or through coercion.

Electronic transactions can facilitate identity theft and fraud because the online process is frictionless and is not always subject to other checks and balances such as responsible lending obligations, which provide oversight and accountability. Electronic transactions, being at arm's length, remove opportunities for creditors or other parties in a transaction to identify warning signs of financial abuse and prevent financial abuse by stopping coerced or fraudulent transactions. Electronic transactions place more of an onus on victim survivors and their advocates to point out and actively prosecute the financial abuse. This in effect reduces the onus on businesses to identify and prevent financial abuse, despite businesses having far greater resources and ability to do so. In recent years, banks have implemented systems and processes to identify warning signs of financial abuse and support victim survivors, including through industry guidelines such as the Australian Banking Association's [Financial abuse and family and domestic violence guidelines](#), and other industries are following.

However, more action is needed from the Government.

---

<sup>1</sup> Deloitte Access Economics (2022) The cost of financial abuse in Australia (Commonwealth Bank of Australia). <https://www.commbank.com.au/content/dam/caas/newsroom/docs/Cost%20of%20financial%20abuse%20in%20Australia.pdf>

<sup>2</sup> Australian Bureau of Statistics, Data and Information Regarding the Personal Safety Survey. In: 4906.0 - Personal Safety Survey Australia 2012. Canberra (AUST): ABS; 2013. Available from: <http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4906.0Main+Features12012?OpenDocument>

<sup>3</sup> Kutin, J., Russell, R. and Reid, M. (2017) 'Economic abuse between intimate partners in Australia: Prevalence, health status, disability and financial stress', *Australian and New Zealand Journal of Public Health*, vol. 41, no. 3, pp. 269-274.

<sup>4</sup> Our Watch (2014) Reporting on family violence in Aboriginal and Torres Strait Islander communities. Melbourne: Our Watch.

Our members primarily see electronic transactions being used to perpetrate financial abuse in two ways: firstly, through coercion, for example where the victim survivor of financial abuse has signed or completed a transaction online under duress or threats of harm from the perpetrator; and secondly, through outright fraud and identity theft, for example where the victim survivor's details have been used online and/or their electronic signature has been forged without their knowledge or consent.

### Case study

Sam\* is very disadvantaged with a history of mental health issues and family trauma. Their partner compelled them to sign loans for their benefit by threatening to leave them, knowing this would leave them homeless. They did not let him work and so they were dependent on Centrelink. On one occasion, they accessed their email account without their knowledge or consent to electronically sign a loan document on their behalf. The loan was for \$6,000 at 28% interest.

\*a pseudonym has been used.

The prevalence of identity theft and fraud has significantly increased in the last few years, corresponding with the growing popularity and use of electronic transactions due to COVID-19 lockdowns. Identity theft complaints to IDCare in Australia involving buy now pay later (BNPL) finance doubled, from 800 reports in 2019 to a record 1,600 in 2020.<sup>5</sup>

### How the ETA currently fails to protect people experiencing economic abuse

The requirement to have documents physically witnessed by an individual provides an opportunity for the witness to confirm the identity of the person signing the document, that the signature was made on the date and location specified, that the declaration was made voluntarily, and that the person making it understood the consequences.<sup>6</sup> This further protects people experiencing financial abuse as it provides a safeguard to victim survivors by providing visibility where duress or coercion is happening, and also ensures that identity fraud can be stopped.

### Case Study

Kelly\* was a stay-at-home mum who lodged her tax returns each year for Family Tax Benefit to be paid. She didn't earn money from any source other than Centrelink, and when she lodged her tax returns, she then received Family Tax Benefit Supplement A. One year after she separated with her ex-husband, she lodged her tax return and didn't receive her supplement. Confused, she contacted the ATO and Centrelink and was advised that her Supplement had been offset against a tax debt and would not be paid to her. Kelly was confused as she had never received any notice of a tax debt and hadn't received any refunds which could have been overpaid.

<sup>5</sup> Byrone Kaye, Australia's BNPL boom pushes identity theft to record, data shows, Reuters, 9 February 2021. Available at <https://www.reuters.com/article/us-australia-bnpl-fraud-exclusive-idUSKBN2A906Q>

<sup>6</sup> Philippa Ryan and Veronica L. Taylor, 'Executing documents in a digital economy: rethinking statutory declarations and deeds in Australia' (September 2021), Available at: <http://regnet.anu.edu.au/research/research-projects/details/8314/how-should-we-modernise-document-execution-australia>

The ATO investigated after their phone call with Kelly, and later explained to her that someone had lodged amended tax returns for four years, resulting in refunds of \$15,000 being paid by cheque. Soon after the amended return amount had been paid via cheque, the ATO had done an internal audit and found that Kelly had not been entitled to the refund and had raised the amount paid out as a debt on her ATO account, which was now accruing interest. Kelly had not made any applications for amended returns, and she was confused how such an application had been made without her knowledge or consent. The ATO explained that the person who did apply must have had access to her personal information including her tax file number and had signed electronically. They were unable to provide her with any more information due to the ongoing nature of the investigation, and Kelly was left confused and unsure of how much of her information was secure, and what steps she should take to protect herself in the future.

\*a pseudonym has been used.

While requiring documents to be witnessed cannot fully protect against coercion, fraud or other challenges faced by people experiencing vulnerability, they do provide an extra safeguard. Often people experiencing financial abuse may have been coerced to share their passwords or PINs with the perpetrator, and the perpetrator may have access to their banking or credit accounts, or authentication methods (such as multi-factor authentication via phone or email) which makes it much easier for fraud to occur in electronic transactions. Where victim survivors are involved in business transactions with the perpetrator, for example as a 'puppet director' or co-director of a family business, the distinction between business and personal transactions may be blurred and the victim survivor may bear personal liability for business transactions, for example where the victim survivor has signed a personal guarantee for a business contract.

Another concern we have is the inconsistency across different state, territory and federal legislation. This is confusing generally, but even more so for people experiencing financial abuse. Different laws regulate electronic transactions in each state, territory and at a federal level.<sup>7</sup>

For example, the form of the statutory declaration is similar and its policy purpose identical across Australian jurisdictions, but the witnessing requirements and the penalties for false declarations are different. One way of addressing the variation across different states and territories would be to ensure mutual recognition of signed documents.

**Recommendations:**

- Legislation, regulations, policies and procedures governing electronic transactions should have added checks and balances in place to protect against financial abuse. For example, this could include a requirement for witnessing. These added checks and balances should be culturally appropriate and accessible.
- Ensure there is harmonisation between state, territory and federal legislation for electronic transactions.

<sup>7</sup> For example, in Victoria are regulated by the *Electronic Transactions Act 2000* (Vic) and the *Oaths and Affirmations Act 2018* (Vic) and in NSW electronic transactions are regulated by the *Electronic Transactions Act 2000* (NSW) and the *Oaths Act 1900* (NSW).

- Ensure mutual recognition of electronic transactions across jurisdictions.

In our experience explaining the effects and consequences of an electronic transaction is beneficial to clients experiencing financial abuse. While they may be able to sign something electronically, they may not have understood it fully. Not all people experiencing financial abuse seek legal advice, as often people do not realise they are experiencing it. Often victim survivors' financial independence is deliberately impeded by perpetrators as a form of abuse, for example by controlling all finances in the household, this means it is incredibly hard for victim survivors to recognise the financial abuse.

**Recommendation:**

Ensure better public awareness around financial abuse and electronic transactions, in particular for marginalised groups, CALD and migrant communities, First Nations communities, specialist domestic violence support workers, and the domestic violence workforce sector.

### Consent requirements

Electronic transactions should have consent requirements and take an 'opt in' approach. This would mean consumers would have the option to participate in electronic transactions.

The EU General Data Protection Regulation (GDPR) and other jurisdictions subsequent to the GDPR's implementation have an 'opt-in' approach to transmission, use and retention of data and information, placing affirmative action in the hands of the consumer.

From the perspective of economic abuse victim-survivors, it is appropriate and reasonable for them to form their own assessment of their financial safety and the integrity of their personal information. They may have valid concerns that their online accounts and data privacy are currently compromised, or a reasonable preference based on past experience.

More broadly, a digital divide is experienced by some victim-survivors, particularly those who have not been afforded digital education and experience prior to arriving in Australia. Their participation in the Australian economy and government systems should not be restricted or disadvantaged by a positive requirement to use electronic transactions where they lack confidence or the skills to do so. Electronic transactions are not accessible to everyone. For example, if people are living in remote areas, they may not have easy access to the internet.

It is also challenging for people experiencing financial abuse to understand legal information that might be required to sign an electronic transaction, even if it is presented in plain language, which is not the case for many electronic transactions.<sup>8</sup> People experiencing financial abuse are often navigating numerous other issues at the same time, requiring a range of legal and social supports, and may not have capacity to process complex information even if it is presented simply. However, ensuring all legal information is

---

<sup>8</sup> Dorothy Ann Fauls, *Plain Language and the Law: Rethinking Legal Information for Vulnerable People in Australia*, (PhD Thesis, University of Queensland, 2018), 83.

presented in plain language will assist consumers in understanding electronic transactions and ensuring consent is properly understood for them to opt in.<sup>9</sup>

Given the prevalence of electronic transactions being used to facilitate financial abuse, there needs to be adequate safeguards focussed on accountability and accessibility to ensure that people understand the financial and legal consequences of electronic transactions, especially for those people with limited financial and digital literacy. In particular, electronic transactions should be opt in and in plain language.

**Recommendation:**

All electronic transactions should be opt in.

**Recommendations**

1. Legislation, regulations, policies and procedures governing electronic transactions should have added checks and balances in place to protect against financial abuse. For example, this could include a requirement for witnessing. These added checks and balances should be culturally appropriate and accessible.
2. Ensure there is harmonisation between state, territory and Commonwealth legislation for electronic transactions.
3. Ensure mutual recognition of electronic transactions across jurisdictions.
4. Ensure better public awareness around financial abuse and electronic transactions, in particular for marginalised groups, CALD and migrant communities, First Nations communities, specialist domestic violence support workers, and the domestic violence workforce sector.
5. All electronic transactions should be opt-in.

---

<sup>9</sup> This could be included in the *Electronic Transactions Regulations 2020* (Cth).