Level 6, 179 Queen Street
Melbourne, VIC 3000

info@consumeraction.org.au
consumeraction.org.au
T 03 9670 5088
F 03 9629 6898

4 October 2024

By email: scamspolicy@treasury.gov.au

Scams Taskforce
Market Conduct Division
Treasury
Langton Cres
Parkes ACT 2600

Dear Director

Scams Prevention Framework – exposure draft legislation

Thank you for the opportunity to provide feedback on the Government's proposed Exposure Draft - Treasury Laws Amendment Bill 2024: Scams Prevention Framework (the Bill) and accompanying Explanatory Memorandum (EM), introducing the Scams Prevention Framework (SPF). This is a joint submission made on behalf of:

- Consumer Action Law Centre
- CHOICE
- The Australian Communications Consumer Action Network
- Financial Rights Legal Centre
- Super Consumers Australia
- Financial Counselling Australia
- WEstjustice

- Consumer Credit Legal Service WA
- Consumer Policy Research Centre

We also support the separate submission of the Australian Communications Consumer Action Network (ACCAN) which sets out ACCAN's concerns with respect to fundamental incentive problems in the SPF which make it impractical and unworkable and concerns regarding the interaction of the SPF and the Telecommunications Act 1997 (Cth).

Our organisations are pleased to have the opportunity to comment on the Federal Government's draft overarching laws to combat scams.

We recognise the challenge of introducing an overarching framework and proposed industry Codes (Codes) across multiple sectors, while scammers continue to innovate, adapt and harm consumers day by day. **The SPF *can* be a world-leading framework, but only if Government recasts the dispute resolution approach** so that the burden is off the consumer and the right incentives exist to drive industry action.

Since providing our feedback[1] to Treasury's December 2023 consultation paper on the Government's proposed scams regulatory framework, our organisations have continued to support innocent, ordinary Australians whose lives have been destroyed by criminal scams. While we have witnessed a handful of businesses taking some steps towards improving security of their systems to prevent scams, this is piecemeal, and there has been almost no improvement or consistency of banks repaying customers for failing to keep their money safe from scammers.

Right now, Australia is a honeypot – the target of scammers domestically and internationally – with more than $2.74 billion lost to scammers last year, that is far more on all measures compared to other countries such as the United Kingdom (UK).[2] Our country's scam response has been left to industry to lead and as a result, it is consumers, not business, that are paying for 96% of scams losses[3] and improvements are far too slow to come online, compared with the rest of the world. The absence of regulation has left Australians exposed to substantial harm. The harm is increasing as scammers become far more sophisticated, adopting artificial intelligence, stealing biometric information and preying on lax security systems in an evolving digital financial system.

Australia has the opportunity within this SPF to aim far higher and become the world leader in preventing and disrupting scams and responding to innocent people and families whose lives are markedly changed by scams. As currently designed, the SPF does not go far enough because:

- it is designed for businesses to take a minimum-standard compliance approach to obligations, rather than incentivising innovation to keep up with scammers who are always steps ahead; and
- the dispute resolution process is unworkable.

If the 'Response' principle were reworked to include a presumption of reimbursement (with limits) and an apportionment mechanism that is business-to-business – this would be world leading, and will significantly reduce both the high number and value of losses from scams, that are wreaking havoc on the lives of countless Australians and their loved ones.

---

[1] See: https://consumeraction.org.au/scams-mandatory-industry-codes-consultation-paper/

[2] National Anit Scams Centre, ACCC. 'Targeting scams: Report of the National Anti-Scam Centre on scams activity 2023'. April 2024. Available at: https://www.nasc.gov.au/reports-and-publications/targeting-scams; UK Finance. 'Annual Fraud report'. June 2024. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024#:~:text=We%20saw%20some%20small%20reductions,and%20the%20number%20of%20cases.; UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/; https://www.afr.com/companies/financial-services/how-an-asic-lieutenant-was-scammed-and-her-warning-for-consumers-20240701-p5jq6d; https://www.theage.com.au/politics/federal/a-scams-bill-that-protects-banks-over-victims-is-the-biggest-scam-of-all-20240919-p5kbt6.html

[3] See: https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-790-anti-scam-practices-of-banks-outside-the-four-major-banks/; https://consumeraction.org.au/report-one-year-on-and-asic-report-again-reveals-banks-shirking-responsibility-when-customers-have-been-scammed/; https://consumeraction.org.au/australias-banks-failing-customers-by-placing-all-the-burden-of-the-scams-crisis-on-them-says-damning-asic-report/

Key Recommendations

1. **Recommendation:** Reframe the 'Response' principle in the SPF to introduce a uniquely Australian reimbursement presumption.
2. **Recommendation:** Support the reimbursement presumption with an apportionment mechanism (to be determined at industry level) to allow businesses to reallocate liability for reimbursed scam losses.
3. **Recommendation:** The new SPF laws should be implemented by mid-2025, with the sector Codes up and running within 8 months of Royal Assent of the SPF.
4. **Recommendation:** The Government to release drafts of the Codes for consultation before the end of 2024.
5. **Recommendation:** The Bill should introduce consumer-centred internal dispute resolution (IDR) where the evidentiary burden lies with SPF entities, which must reimburse the consumer in a timely manner.
6. **Recommendation:** The SPF Bill must be more prescriptive to place a higher bar on businesses to prevent, detect, disrupt and respond to scams in the Codes, including through greater incentives for businesses to invest in technology and security systems, rather than rely on warnings and minimum obligations to protect consumers.
7. **Recommendation**: Introduce an overarching goal and provisions in the Bill that require businesses to do more to protect consumers experiencing vulnerability and disadvantage from scams. The EM should also provide examples of the higher bar placed on businesses to identify customers experiencing vulnerability, address their extra need, and protect them from scams.

Other Recommendations

8. **Recommendation:** Short of reimbursement, the Bill must signpost that the SPF entity which is first notified by a consumer of a scam must join all possible parties they expect to share liability into an SPF complaint to reduce the burden on scam victims.
9. **Recommendation:** Scam victims who make reports should only have restriction or disruption to their own services in exceptional circumstances, and for the least amount of time. Thought should be given to a simple process for victims to access help if their account or services are frozen.
10. **Recommendation:** Minimum standards and greater use of guidance notes with examples in the Bill and EM on what 'reasonable steps' and other reasonableness tests would look like should be enshrined in the Bill to set up the strongest possible sector Codes.
11. **Recommendation:** The SPF must include a consumer-focused standardised IDR timeframe across all SPF sectors no longer than 10-20 days, under a 'no wrong door IDR principle' incorporated in the SPF Bill.
12. **Recommendation:** The external dispute resolution (EDR) process must incentivise fair settlement by businesses at IDR.

Other Recommendations (continued)

13. **Recommendation:** Disputes must be automatically escalated to the Australian Financial Complaints Authority (AFCA) by businesses if a consumer is dissatisfied with an IDR resolution.
14. **Recommendation:** AFCA should be able to impose extra fees and increase levies on SPF entities who are found to have engaged in poor conduct or who regularly leave scam victims to turn to EDR.
15. **Recommendation**: AFCA should be empowered to require banks to automatically halt interest being charged on disputed scam transactions and impose debt waiver determinations on credit funds that have been lost to a scammer.
16. **Recommendation**: 'Actionable scams intelligence' must be easily accessible via the Australian Financial Crimes Exchange (AFCX) in a way that reasonably minimises information asymmetries for the consumer.
17. **Recommendation:** Actionable scams intelligence must not be restricted by privacy arguments.
18. **Recommendation:** The SPF Bill or Codes should prohibit confidentiality and non-disparagement clauses and all forms of non-disclosure agreements (NDAs).
19. **Recommendation:** The SPF must set stronger measures to stop mule and fraudulent accounts being used to perpetrate scams, and introduce meaningful penalties for banks that allow the opening and operation of scam mule accounts on their platforms.
20. **Recommendation:** Strengthen s58BK 2(a) to require businesses to do more than only identify and provide warnings to consumers at a higher risk of scams.
21. **Recommendation:** Strengthen s58BD to require banks to proactively monitor transactions – and provide more detailed actions and examples in this respect in the EM.
22. **Recommendation:** Tier one penalties must be available for all Code breaches, or at least systemic Code breaches, and the penalty specified for infringement notices under s58FN must be significantly increased.
23. **Recommendation:** The ACCC should be funded to undertake an independent review of the SPF after 18 months of its operation, with a focus on outcomes of consumers experiencing vulnerability and disadvantage.
24. **Recommendation:** The SPF Bill to make clear that the SPF, and the SPF Banking Code is in addition to, and not in derogation of, the rights of a customer under the ePayments Code, who must also have an easier and streamlined pathway to redress than currently under the ePayments Code.
25. **Recommendation:** Future sectors, including superannuation, are designated within 8 months of Royal Assent. Government should commit to this timeframe by documenting it in the EM and parliamentary speeches.

Please contact Policy Officers **Rose Bruce-Smith or David Hofierka** at **Consumer Action Law Centre** on 03 9670 5088 or at david.h@consumeraction.org.au if you have any questions about this submission.

CONSUMER ACTION LAW CENTRE

Stephanie Tonkin | CEO

CHOICE

Rosie Thomas | Director, Campaigns and Communications

THE AUSTRALIAN COMMUNICATIONS CONSUMER ACTION NETWORK

Carol Bennett | CEO

FINANCIAL RIGHTS LEGAL CENTRE

Karen Cox | CEO

SUPER CONSUMERS AUSTRALIA

Xavier O'Halloran | CEO

FINANCIAL COUNSELLING AUSTRALIA

Dr Domenique Meyrick | Co-CEO

Peter Gartlan | Co-CEO

WESTJUSTICE

Joseph Nunweek | Legal Director, Economic Justice Team

CONSUMER CREDIT LEGAL SERVICE WA

Roberta Grealish | CEO (Acting)

CONSUMER POLICY RESEARCH CENTRE

Erin Turner | CEO

TABLE OF CONTENTS

About Consumer Action

Consumer Action Law Centre (CALC) is an independent, not-for profit consumer organisation with deep expertise in consumer and consumer credit laws, policy and direct knowledge of people's experience of modern markets. We work for a just marketplace, where people have power and business plays fair. We make life easier for people experiencing vulnerability and disadvantage in Australia, through financial counselling, legal advice, legal representation, policy work and campaigns. Based in Melbourne, our direct services assist Victorians and our advocacy supports a just marketplace for all Australians.

About CHOICE

CHOICE is the leading consumer advocacy group in Australia. CHOICE is independent, not-for-profit and member-funded. Our mission is simple: we work for fair, just and safe markets that meet the needs of Australian consumers. We do that through our independent testing, advocacy and journalism.

About the Australian Communications Consumer Action Network

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers.

About Financial Counselling Australia

Financial counsellors assist people experiencing financial difficulty by providing information, advice, support and advocacy. Working in not-for-profit community organisations, financial counselling services are free, independent and confidential.

Financial Counselling Australia (FCA) is the national voice of the financial counselling profession in Australia. We are a not-for-profit organisation that: Provides resources and support for financial counsellors; Advocates to increase access to financial counselling; Works to raise the profile of financial counsellors; Advocates for a fairer marketplace; and Works to improve hardship processes for people in financial difficulty. FCA also co-ordinates the National Debt Helpline (NDH) and runs The Small Business Debt Helpline (SBDH).

About Financial Rights Legal Centre

Financial Rights is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Finally we operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies.

About WEstjustice

WEstjustice provides free legal services and financial counselling to people who live, work, or studying in the cities of Wyndham, Maribyrnong and Hobsons Bay, in Melbourne's western suburbs. We have offices in Werribee and Footscray, as well as youth legal branch in Sunshine, and outreach across the west. Our services include: legal information, advice and casework, duty lawyer services, community legal education, community projects, and law reform and advocacy.

About Consumer Credit Legal Service WA

CCLS champions the financial rights of Western Australians on credit, debt and consumer law issues.

- We ensure people in Western Australia are treated fairly in the financial marketplace by providing free, confidential legal advice through our Telephone Advice Line.
- We provide legal representation to
- people experiencing vulnerability and disadvantage so that they can access justice.
- Our community legal education programs empower West Australians experiencing vulnerability and disadvantage to understand their rights and avoid financial pitfalls.
- We help other service providers, including financial counsellors and community support workers, to understand and support their clients' financial rights.
- We are a voice for change so that financial systems and consumer laws are improved for all.

About Consumer Policy Research Centre

The Consumer Policy Research Centre (CPRC) is an independent, not-for-profit, consumer think tank. CPRC aims to create fairer, safer and inclusive markets by undertaking research and working with leading regulators, policymakers, businesses, academics and community advocates.

About Super Consumers Australia

Super Consumers Australia is the people's advocate in the superannuation sector.

Super Consumers Australia advances and protects the interests of people on low and middle incomes in Australia's superannuation system. It was founded in 2013 and received funding for the first time in 2018.

Executive Summary

Australians are being scammed out of billions of dollars every year. Scams are wreaking financial havoc on our community, causing mental distress to thousands of Australians, and undermining trust and confidence in our financial systems. Scams are a human problem – the immense cost to consumers must drive the Government's response.

Urgent action is required to establish an effective consumer protection framework that prevents, detects, disrupts and responds to scams and addresses the harms being done.

Australia needs a scams framework that places the consumer front and centre of its design. This means creating a regime that – at every step – incentivises those institutions who control the tools fundamental to engaging in a modern economy (our banks, payment system, communications and social media platforms) to prevent, detect and disrupt scams. It also means developing a regime that empowers victims of scams to seek and obtain appropriate redress in a fast and straightforward fashion that causes them no further harm.

We recognise the challenge of introducing an overarching framework across multiple sectors, while scammers continue to innovate, adapt and harm consumers day by day. **The SPF *can* be a world-leading framework, but only if Government recasts the dispute resolution approach** so that the right incentives exist to drive industry action and response.

As shown in the Journey Map at Appendix A, **a 'Modified Reimbursement Framework' that we propose would reduce the scam complaints process from potentially two years under the proposed SPF to just two to three weeks**. It also has benefit of apportioning mandatory reimbursement across digital platforms and telcos.

The proposed SPF places a heavy burden and system stacked against consumers

The proposed SPF 'Response' stage places the onus on an already vulnerable consumer to take on their bank, telco and/or social media platform to prove that the institution did not meet the requirements of the SPF. This is the reverse of the current situation under the ePayments Code, where there is a presumption to assist consumers to argue against large corporations that the scam was not their fault.

This onus reversal introduces a complex, legalistic, time and resource-draining task for the consumer. This task will be all the more difficult since the consumer is often prevented from gaining access to the evidence required to support a case against an institution. Whether an institution has acted on 'actionable scam intelligence' or met their required 'reasonable steps' will be off-limits information to the consumer.

Consumers without the assistance of experienced advocates (or even with them) will continue to fall through gaps and pay for a system set up with business interests at the front. Based on our experience assisting scam victims, we are concerned that the SPF risks setting up a system for businesses to do the minimum required to protect people from scams. If businesses can simply assert that they broadly complied with the policies, procedures and obligations required under the SPF and the Codes, scammed consumers will not be in a position to engage with all the complex legal arguments that internal dispute resolution (IDR) will require. Instead, they will find themselves pitted against well-resourced multi-national corporations such as Meta and Google, or a major bank or telco. We

see this dynamic and general 'tick-a-box' compliance, or even serous non-compliance in other areas[4], including financial services such as banking and insurance regularly already.

Rather than incentivising our institutions to do all they can to prevent scams, the proposed SPF 'Response' will perversely:

- make it likely that consumers give up early in the face of a prospective 2+ years of fighting ahead of them;
- make it likely consumers to accept early lowball offers for restitution; and
- allow institutions to simply assert that they have met the requirements of the SPF in many cases.

The Government needs to reconsider the proposed SPF to better serve consumers and to mitigate harms being done to them.

Reimbursement for scam victims must be at the heart of the scams regulatory framework

The SPF 'Response' stage needs to be amended to introduce a Modified Reimbursement Framework – a model overwhelmingly supported by the Australian public.[5] A presumption of bank reimbursement **can** sit within these draft laws and represents an opportunity for Australia to take a world-leading, evidence-informed approach to dispute resolution and incentivise industry responses.

A Modified Reimbursement Framework would include:

- a presumption of reimbursement for scam victims at IDR;
- an apportionment mechanism for liability of scam loss between SPF businesses (SPF entities); and
- appropriate limits, including for gross negligence and fraud.

Apportionment of liability is only workable **after** a victim is reimbursed. Apportionment must be worked out business-to-business according to agreed default liabilities – in the same way insurance companies have agreed at an industry level shared apportionment of liability, without the need for the consumer to chase multiple drivers and insurers of a multi-car accident.

An SPF with a modified reimbursement framework will:

- decrease costs to business having to resource IDR, external dispute resolution (EDR) and long legal battles;
- reduce expected costs to EDR vis-à-vis the current proposal; and
- alleviate the burden on consumers to seek redress in terms of time, resources and mental health.

A Modified Reimbursement Framework will establish the necessary incentives into the system to motivate our institutions to take stronger actions under the prevent, detect, report and disrupt steps of the SPF. It would build on, complement and support many of strongest aspects of the proposed reforms that have already been included in the Bill:

- a single door EDR system through the Australian Financial Complaints Authority (AFCA); and
- oversight through empowered scam regulators led by the Australian Competition and Consumer Commission (ACCC), supported by fast scams reporting requirements and a robust penalties framework.

[4] See: https://bankingcode.org.au/resources/bccc-report-compliance-with-the-banking-code-of-practice-july-to-december-2023/; https://insurancebrokerscode.com.au/ibccc-publishes-its-2023-annual-data-report/; See: https://consumeraction.org.au/the-telco-code-has-run-its-course-and-failed-to-deliver-acma-must-explore-other-options-to-protect-consumers/

[5] See: https://consumeraction.org.au/polling-big-majority-of-australians-say-banks-should-do-their-job-and-take-responsibility-for-keeping-our-money-safe/

Prevention, detection and disruption measures should reduce the scale of scam losses and reduce the "reimbursement bill" over time, but a level of reimbursement must be incorporated into the framework for efficiency, and to cope with the unmanageable caseloads of scam complaints to come.

Timeframes slow while Australians continue to lose billions to scams

There must be a clear commitment to a timely designation of other relevant sectors under the SPF, including superannuation, crypto, online marketplaces and other digital, financial and on-line sectors and businesses.

Finally, it is imperative that the proposed framework is implemented as soon as is practicable. The framework is desperately needed and the timeframes for writing and implementing the first three Codes must also reflect this urgency – this could be reflected in the Bill or at least the EM.

The Government must re-consider the proposed SPF to include a Modified Reimbursement Framework and fast track its passage through parliament for implementation as soon as possible. Action is needed now to introduce an effective regime to protect Australians from scams.

1. A strong Scams Prevention Framework (SPF) needs to be prioritised, with positive aspects welcomed

- Principles-based obligations a good approach, but more detail needed
- A broad scam definition
- Definition of SPF consumer
- Single door EDR through AFCA is a good approach
- Empowered regulators and high tier one penalties
- Safe harbour provisions

Principles-based obligations a good approach, but more detail needed

Although there remains a lot yet to be determined in the SPF – at a high level, we support the principles-based approach which underpins the broad framework.

The SPF is a well-intentioned, genuine and welcomed reform introduced by Government, setting the scene for meaningful scam protections.

Many provisions in the SPF to assist consumers and business would serve as a welcomed uplift compared to the absence of scam protections Australian are currently afforded. However, the SPF could go further with an overall higher standard of consumer safeguards, particularly in dispute resolution, to work for consumers in practice and drive the best incentives to combat scams.

Although a customer could be forgiven into thinking these measures are already in place across the board, the SPF Bill and EM provide some discrete examples of specific actions SPF entities would be expected to take to protect consumers. Banks for example, would need to develop processes to flag and add friction such as 24 hour holds to high risk and high value transactions that appear out of character, or a pause authorised push payments while it is investigating a substantial number of similar reports of suspected scams. But in the draft documents, these examples are far and few between.

Some other necessary scam prevention measures under development, prompted and accelerated due to the proposed SPF, including the proposals to mandate confirmation of payee for banks as part of the Scams Safe Accord[6], and an SMS ID registry for telcos, will play a crucial role in combatting scams (although their timing and commencement remain uncertain). Banks would also need to provide additional technology that consumers can access to stop scams such as account freeze switches.

But as we discuss throughout this submission, without clearer prescriptive guidance in the Bill informing and setting expectations for the SPF and Codes, there will be too much latitude for business to do the bare minimum, and even fewer arguments that consumers affected by scams could rely on to obtain redress and a fair outcome.

A broad scam definition

We support the adjustment to the definition that clarifies that the consumer does not need to prove the 'intent' on behalf of the scammer. However, we recommend further clarifying the rationale and meaning of the reference at paragraph 1.78 of the EM to potentially exclude 'cybercrime' from the definition of a scam, as we would not want to see this unsuitably limit the Bill's coverage. We also see a number of cases where scammers use significant social engineering to manipulate people, such as in romance scams. The higher standard the law requires to prove deception, as opposed to e.g. 'misleading' may serve to exclude some circumstances from the SPF scam definition.

[6] See: https://www.ausbanking.org.au/scam-safe-accord/

We recommend that consideration be given to whether the relevant test should incorporate circumstances where a consumer was 'misled'.

Definition of SPF consumer

We support the definition of SPF consumer which will provide the right for scam victims to initiate complaints and seek redress against all SPF entities associated with a scam. This includes SPF entities that do not have a contractual relationship with the SPF consumer, and regardless of whether an SPF entity knew about the SPF consumer. This is essential to ensure the proper functioning of the SPF.

Single door EDR through AFCA is a good approach

We support the establishment of a single-door EDR scheme, where AFCA will have jurisdiction to deal with all scam disputes involving banks, telcos and digital platforms. We stress the importance of maintaining the simplest dispute resolution pathway for consumers as the SPF expands to cover more jurisdictions. To maintain the single door, there may be circumstances requiring co-opting of specialist expertise from other sectors such as the Telecommunications Industry Ombuds (TIO) scheme. This should happen behind the scenes through arrangements between the Ombuds schemes.

Empowered regulators and high tier one penalties

We support the proposed designation of the ACCC as the SPF general regulator to oversee and enforce the regime, co-ordinate with others to identify emerging and systemic trends causing consumers the most harm, and support actionable scam intelligence being passed on quickly throughout all relevant areas of the scams ecosystem that will hopefully prevent and lead to a reduction to the harm from scams.

We also welcome the tier one civil penalty provisions up to $50m, or through penalties linked to the benefit obtained for SPF breaches, or as a percentage of turnover that appropriately reflect the gravity of SPF entities failing to meet the SPF principles. But as we outline below, penalties are a fraction of an effective regulatory framework. More depth in penalty provisions is needed to prevent widespread harm (Part 6 below) and dispute resolution is the touchpoint for scam victims, that needs to work efficiently and effectively (Part 3 below).

Safe harbour provisions

The safe harbour provisions appear appropriate to ensure businesses can respond to scams promptly, but we need to ensure they do not negatively impact on consumers who have been victimised by a scam. The time limit of 28 days and the test of 'reasonableness' is a good minimum safeguard, but the EM should go further to outline the limits of 'reasonableness' to minimise disruption to consumers. It is unclear what overarching obligations will apply to SPF entities to minimise disruption to a consumer themselves when there is reasonable suspicion that their account is at risk or possibly compromised.

We are aware of an instance where a victim's bank sent a recall request to the receiving bank, who froze the compromised account. The *scammer* then lodged an AFCA complaint which resulted in the release of the stolen funds. This is an unacceptable outcome and we are pleased the SPF intends to prevent these outcomes. But we have also heard from many people whose accounts were frozen for unacceptable periods of time after they reported losing money to a scam. Being unable to receive wages, or put money in an offset account, compounds the harm of a scam.

Consideration also needs to be given to the telco and digital platform sectors – and others to be regulated down the line – to minimise harm for consumers who are victimised by a scam. Particularly, suspending a customer's telephone service should only be acceptable in extreme circumstances. We believe that there should be an overarching confirmation that scam victims who make reports only have restriction or disruption to their own

services in exceptional circumstances, and in these circumstances for no longer than 48 hours. In circumstances like these, consumers will need a simple way to get support and access to their funds and essential services.

Key Recommendation

The SPF Bill must be more prescriptive to place a higher bar on businesses to prevent, detect, disrupt and respond to scams in the Codes, including through greater incentives for businesses to invest in technology and security systems, rather than rely on warnings and minimum obligations to protect consumers.

Recommendation

Scam victims who make reports should only have restriction or disruption to their own services in exceptional circumstances, and for the least amount of time. Thought should be given to a simple process for victims to access help if their account or services are frozen.

2. A Uniquely Australian Reimbursement Model – simple and world-leading

- Australia can introduce a world-leading, simple and effective response to scams
- Journey Map illustrate the SPF Response approach is unworkable and stacked against the consumer
- Apportionment of losses after victim is reimbursed, business-to-business
- Why bank reimbursement?
- The UK model is working, and we can improve on it

Australia can introduce a world-leading, simple and effective response to scams

The focus of the SPF is on industry preventing scams. However, scammers are sophisticated criminals. They will always find gaps and weaknesses in preventative systems to steal money—scammers are highly proficient and there are lucrative incentives to keep on innovating and finding new ways to scam victims.

Australia could incentivise the best scams prevention system in the world by recasting the 'Response' principle in the SPF into a 'Modified Reimbursement Framework'. Dispute resolution is fundamental to how well the SPF can work because it drives the incentives of the whole system.

Uniquely Australian Reimbursement Model that will lead the world on scams disruption and response

- Presumption of bank reimbursement
- Consumer provides reasonable information to the bank
- 10 business days for a bank to respond and reimburse, in most cases
- Limits to the presumption may exist: gross negligence, knowingly taking part in the fraud
- Single door EDR at AFCA if reimbursement refused
- Apportionment *after* a consumer is reimbursed, business-to-business
- Apportionment agreed at an industry level between SPF entities, highly efficient

The Modified Reimbursement Framework can sit within the SPF Response principle. It would incentivise industry to find efficiencies and default positions for apportionment sooner. This will mean:

- Dispute resolution will be workable, streamlined and more cost-effective, including for businesses, who could pay more in dispute and legal costs than the "reimbursement bill";
- The party best placed and resourced to mitigate scams risk (business, not consumer) is incentivised to prevent scams;
- Victims won't bear the cascading financial and mental health harms that happen after a scammer has stolen their life savings;
- Businesses and sectors flying under the radar of very high-level obligations with a single regulator are still incentivised to prevent and disrupt scams; and
- The framework contains efficient timeframes, limits and ensures fairness.

Journey Map illustrate the SPF Response approach is unworkable and stacked against the consumer

At Appendix A we have mapped out a hypothetical example of a consumer journey through the proposed dispute resolution system in the SPF. While we can only make assumptions about the process and how AFCA might design the dispute resolution process at EDR, we know the SPF places the onus on the consumer and creates a case-by-case compensation and apportionment model. We can also draw on our many years representing scam victims through dispute resolution to map out a plausible journey. Without significant overhaul, we are deeply concerned the SPF dispute resolution system will be unfair and unworkable.

Under the SPF, a scam victim will only be entitled to compensation for a proportion of loss or damages after demonstrating a SPF entity has failed to meet a relevant standard, after potentially lengthy IDR and EDR processes or via expensive court action. Based on our casework experience, it will almost certainly take many months and sometimes years for a complaint to track through the SPF dispute resolution process, which is stacked against the consumer through information asymmetry, confidentiality provisions and industry practices we see now: banks denying liability at early stages of dispute resolution and making low settlement offers, even in cases where under current laws they are later found to be fully liable for a scam.

Imposing the SPF obligations – and liability for failing to meet them – on digital platforms will be world leading (a model that even UK banks have been calling for)[7]. The obligations are novel and complex across the banking and telecommunications sectors as well. But the SPF includes them in a system that is adversarial in nature and places the impossible burden on a consumer to make complex legal arguments against some of the largest multinational companies in the world. It sets up dispute resolution to be a David and Goliath battle, hard fought every time someone asks for compensation from the businesses that failed them.

We know that the status quo of fighting banks at IDR and EDR and making arguments under the Banking Code of Practice, ePayments Code and Corporations Act is exhausting and difficult. Scam victims tell us it's like having a second job – they're victims of crimes only a bank can prevent, yet they are treated like the criminal. One lawyer representing victims to final determination at AFCA told us that virtually every complainant needs an experienced commercial lawyer to have a real chance of success.

Key Recommendation

Reframe the 'Response' principle in the SPF to introduce a uniquely Australian reimbursement presumption.

Apportionment of losses after victim is reimbursed, business-to-business

Apportionment of scams losses across industry will incentivise investment in combatting scams and Australia is taking a leading step of drawing telcos and digital platforms into the regime. However, the Journey Map illustrates that apportionment of a 'simple scam' may be entirely unworkable if determined on a case-by-case basis while the victim awaits an outcome on their complaint. Apportionment of scam losses is only workable and fair if it occurs after a consumer has been compensated, between businesses (although the consumer can be required to co-operate and to provide relevant information to assist with bank investigations).

The SPF has an opportunity to go a step further than the UK model, and outline some broad principles to set liability and apportionment from the start, including:

- A presumption of bank reimbursement;

[7] See: TSB hits out as social media fraud redress plan is dropped (ft.com)

- Other businesses to repay their apportionment contributions to the bank after the bank repays the consumer; and
- Setting or requiring sectors to agree to apportionment defaults that will be binding at IDR and EDR – e.g. Telco letting a scam text through = 30%, receiving bank hosting mule account = 40%, sending bank = 30%

Key Recommendation

Support the reimbursement presumption with an apportionment mechanism (to be determined at industry level) to allow businesses to reallocate liability for reimbursed scam losses.

Why bank reimbursement?

The sending bank needs to reimburse the scam victim at first instance for several important reasons:

1. The consumer will almost always go to their bank for help when they have lost money from that bank account.
2. The consumer may not know the other entities involved in the scam that may be liable.
3. Banks are most developed in dispute resolution and resourced to make the payment at first instance.
4. If businesses just agree to a set proportion to each pay the consumer, the consumer is left chasing up the payment and this could be an impossible task.
5. Banks have significant leverage and resources to negotiate the fair shared liability amounts behind the scenes with digital platforms and telcos, as opposed to a scam victim with limited financial resources.

The UK approach is working – and we can improve on it

The United Kingdom has identified that the simplest way to incentivise banks to prevent scam losses and provide redress to victims was a reimbursement model. This was decided with consumers needs front and centre, with significant inbuilt features to protect those experiencing vulnerability and disadvantage.[8]

The UK reimbursement model is set to become mandatory in October 2024 testament to the voluntary reimbursement framework in force now **working** – losses from authorised and unauthorised fraud are on the decrease.[9] In 2023, UK banks taking part in the voluntary code on average reimbursed approximately 67% of money lost to scams, with some banks refunding almost 90%.[10] The UK's reimbursement cap has been finalised at £85,000 which will cover an estimated 99% of scam claims. [11] A review will be conducted in 12 months. In contrast, Australia's banks compensate just 2-7% of scam losses.[12]

UK banks are ahead of Australia in implementing leading scams technology, including confirmation of payee, that is also already up and running in other parts of Europe, and New Zealand will be introducing it by the end of this year[13]. UK Finance publicly states that the "efforts applied by UK banks have had a positive impact on fraud," with

[8] See: https://www.psr.org.uk/media/as3aoxan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf;https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/app-fraud-uk/
[9] UK Finance. 'Annual Fraud report'. June 2024. p.10. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024#:~:text=We%20saw%20some%20small%20reductions,and%20the%20number%20of%20cases.
[10] UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/
[11] See: https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-its-decision-on-app-scams-reimbursement/#:~:text=Today%2C%20the%20PSR%20has%20confirmed,Payments%20will%20be%20%C2%A385%2C000.
[12] https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-790-anti-scam-practices-of-banks-outside-the-four-major-banks/.
[13] See: https://www.abc.net.au/news/2024-09-20/australia-scam-draft-law-banks-telco/104361546

both authorised and unauthorised fraud trending down.[14] The simple reason why prevention technology was brought online in the UK and Europe quickly, is that the banks are on the hook (or soon to be) to reimburse scam losses. This demonstrates the clear incentive that a presumption of bank reimbursement drives action in preventing scams. In Australia, confirmation of payee technology is still being built, despite existing elsewhere across the world, and meanwhile Australians are losing large, preventable amounts of money to invoice scams with no recourse.

While Australian banks have been arguing that a reimbursement model will make us the 'honeypot' for international scams, the reality is clear – we are already a prime target, with losses exceeding the UK in monetary value, let alone per capita or per minute.[15]

"*Unlike in the UK, many countries are experiencing an increase in most types of fraud, especially scams. The US recorded staggering losses of US 10 billion, and Australia, a country of just 26 million people, recorded AUD 3 billion in APP losses*"[16] – UK Finance

Other countries are fast moving towards a UK style reimbursement model, such as New Zealand[17] and Thailand[18]. In the US, 75% of large banks have also agreed to reimburse victims of authorised fraud (scams).[19] Australia differs from the UK and other countries in extending scams legislation beyond the banking sector and requiring digital platforms to take action to prevent and disrupt scams. We understand that a cross-sector data sharing regime to be established in the SPF – currently partially in effect through NASC and the AFCX – also has the potential to go a long way beyond the UK reporting framework, although we are concerned about how long this might take to materialise.[20]

[14] UK Finance. 'Annual Fraud report'. June 2024. p.10. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024#:~:text=We%20saw%20some%20small%20reductions,and%20the%20number%20of%20cases.
[15] https://www.theage.com.au/politics/federal/a-scams-bill-that-protects-banks-over-victims-is-the-biggest-scam-of-all-20240919-p5kbt6.html
[16] UK Finance. 'Annual Fraud report'. June 2024. Available at: UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. p.25. Available at: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024#:~:text=We%20saw%20some%20small%20reductions,and%20the%20number%20of%20cases.
[17] See: https://www.nzba.org.nz/2024/04/15/banks-seek-government-support-for-anti-scam-centre/
[18] See: https://aseannow.com/topic/1325369-thai-ministry-to-reimburse-victims-of-call-centre-scams/?fbclid=IwZXhobgNhZW0CMTEAAR2jwVlN6VpVRfZCQeUJSBZKQk40LCechEZUARZpIn34BxJzQEbvEGh3ZVo_aem_Aaf7BVt-orTg8vOCyii5o99yCjcmMowoNC4uwtZmmfzxoY_MuUcgSDI8gniqhCJUecfRcUyULK_dCc6gkmHXP7dz
[19] Available at: https://www.pymnts.com/news/security-and-risk/2024/75percent-large-banks-agree-reimburse-victims-authorized-fraud/
[20] See: How data sharing can protect victims and prevent fraud - Which? Policy and insight

3. SPF Response – Dispute Resolution will be unworkable

A. Internal Dispute Resolution

- IDR across multiple businesses, scams victims falling through the gaps
- Reasonableness tests
- Obligations overseen by a regulator don't replace the need for effective dispute resolution
- Information asymmetry stacks the system against consumers
- SPF IDR must give consumers confidence and certainty and set strict timeframe limit on businesses
- Poor industry conduct toward consumers and power imbalance will carry over to the SPF

B. External Dispute Resolution

- Single door EDR through AFCA is good but still an impossible burden on consumers
- Apportionment unworkable case-by-case at EDR
- The EDR process must incentivise settlement at IDR

C. Transparent information sharing, including via AFCX

D. Resource implications for community lawyers and financial counsellors

A. Internal Dispute Resolution

IDR across multiple businesses, scams victims falling through the gaps

The SPF establishes that regulated businesses must have accessible and transparent IDR for scams disputes, but leaves further details about how it will operate under the sector Codes. We understand from our discussions with Treasury that the intention is that a consumer can lodge a dispute with any business related to the scam they experienced, and will be able to escalate to EDR following a decline from any IDR. The EM at paragraph 1.200 foreshadows that the Codes may prescribe 'cooperation requirements' but it is unclear what these might look like. In the absence of requirements to share information and liability between businesses at IDR, no business at IDR will be able to make a decision that is satisfactory to either the business or the consumer.

Our casework and the Australian Securities and Investments Commission's (ASIC) scams reports show that businesses have very inconsistent approaches to scam prevention and response.[21] Disharmony in approaches to preventing and responding to scams will make cooperation at IDR between businesses very unlikely under the SPF. Without pre-agreed apportionment at an industry level, we believe the vast majority of disputes will be escalated to EDR and the volume will put entirely unmanageable pressure on AFCA. This will not only increase demand on the scarce resources and time constraints that community legal organisations are already facing, it will divert resources away from immense demand for our other services in a cost of living crisis.[22]

[21] See: https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-790-anti-scam-practices-of-banks-outside-the-four-major-banks/; https://consumeraction.org.au/report-one-year-on-and-asic-report-again-reveals-banks-shirking-responsibility-when-customers-have-been-scammed/; https://consumeraction.org.au/australias-banks-failing-customers-by-placing-all-the-burden-of-the-scams-crisis-on-them-says-damning-asic-report/

[22] Consumer Action Law Centre. March 2024. 'At the front line of the cost-of-living crisis: Insights from a Telephone Financial Counselling Helpline'. Available at: https://consumeraction.org.au/report-at-the-front-line-of-the-cost-of-living-crisis/

Disputes under the SPF with multiple respondents may end up looking like high-cost commercial litigation. It is unlikely the consumer's interests will be put front and centre. At a minimum, as illustrated in the Journey Map at Appendix A, there are likely to be claims against the customer's bank (if they only have one), the receiving bank, and at least one telco and digital platform. We frequently speak with consumers where there are upwards of 5 businesses involved in the scam – that we can identify. An empowered scams EDR scheme may find more.

A robust framework outlining the operation of multi-business IDR needs to be enshrined in the SPF, not left to the Codes. This includes referencing liability in the wording of the Response principle and requiring banks to join all possible parties they expect to share liability into a complaint to reduce the burden on scam victims. If a victim seeks help from a non-bank SPF entity, there should be a requirement for all non-bank SPF entities to immediately join the relevant banks to proceedings. This must be signposted by the Bill from the start, as some SPF industries have no or very immature IDR processes compared to the banking industry.

A presumption of reimbursement would resolve most scam matters at IDR, and streamline and avoid many of the issues mentioned above, and then only a limited number of complex cases would proceed to EDR.

Key Recommendation

The Bill should introduce consumer-centred IDR where the evidentiary burden lies with SPF entities, which must reimburse the consumer in a timely manner.

Recommendation

Short of reimbursement, the Bill must signpost that the SPF entity which is first notified by a consumer of a scam must join all possible parties they expect to share liability into an SPF complaint to reduce the burden to scam victims.

Reasonableness tests

Under the SPF, harm from scams will largely depend on what positive actions businesses will have to take to protect consumers. At both IDR and EDR, these actions and the test about whether a business has complied with its obligations under the SPF turn on the question of whether an SPF entity took 'reasonable steps' at the time of the scam. For example, if an SPF entity asserts it has met the reasonable steps requirements, such as to prevent and detect scams under s58BJ and s58BN, how will a consumer rebut the assertion that the SPF entity did 'identify the classes of SPF consumers who have a higher risk of being scammed'? Is it determined by what the industry is doing? For example, if the major banks are imposing a 24-hour delay on first time payees, is that that the standard? Or is it unreasonable not to identify simultaneous Australia and overseas logins at the same time?, or not detect a scam when the credit limit is significantly increased prior to a payment to a first time payee?

Similar difficulties surround the ambiguity in the SPF on what would constitute 'reasonable grounds' before SPF entities would need to act on and disclose 'actionable scam intelligence' under s58AI. It is even arguable that the requirement to take reasonable steps within a 'reasonable time' under s58BW could be a lower standard than current obligations by banks, where it is generally expected that they take steps immediately once they have discovered a scam.

The success of the SPF is far too important for the interpretation of key SPF protections in it to be left solely to go through future consultations on the sector Codes, or risk being watered down further down the track. Even with some of the examples provided, the drafting allows for too many ways that could limit the obligations of businesses under the Codes. For example, we do not agree that it should take a 'substantial' number of scam reports to require SPF entities to take further reasonable steps under the SPF as currently referenced in s58BW(3). Every scam report should trigger extra obligations under the SPF in a proportionate manner, and should constitute 'reasonable grounds' to pass on actionable scams intelligence. Red flag processes must also be developed for all

out of character transaction, not just 'high risk' transactions as many scams intentionally and regularly involve smaller transactions to evade detection.

The SPF needs to do more than require businesses to go little beyond what they already should have been doing years ago.

Minimum standards and greater use of guidance notes with examples in the Bill and EM on what 'reasonable steps' and other reasonableness tests would look like should be enshrined in the Bill to set up the strongest possible sector Codes.

Recommendation

Minimum standards and greater use of guidance notes with examples in the Bill and EM on what 'reasonable steps' and other reasonableness tests would look like should be enshrined in the Bill to set up the strongest possible sector Codes.

Obligations overseen by a regulator don't replace the need for effective dispute resolution

The ongoing reluctance of major corporations to make greater efforts to follow requirements and report under existing Codes[23] and compliance regimes, also show many are simply not compelled or willing to take the steps needed to make their processes easier for consumers if there are no strong incentives in place, or harsh consequences that will impact their bottom line. For example, the Insurance Brokers Code Compliance Committee (IBCCC) has called for improved reporting and transparency among insurance brokers after a 48% increase in breaches[24]. Similarly, the Banking Code Compliance Committee's (BCCC) recent report found a 58% increase in complaints handing breaches under Banking Code of Practice.[25] With no strong incentive, many of these firms currently do not report breaches of their Code.

While the SPF response to this kind of practice is to resource regulators and oversight bodies to better monitor and enforce conduct and compliance – almost all businesses will fly under the compliance radar, given the sheer numbers of regulated entities that will be subjected to the SPF, and the breadth in scale of breaches that will occur (from low level breaches that will likely be left alone, through to systemic that may be dealt with). Large and well-resourced SPF entities will also fight to limit their liability to the detriment of smaller operators joined to the same scam dispute. Ultimately, the consequence will be greater demand and pressure at dispute resolution and an uphill battle for scam victims.

Information asymmetry stacks the system against consumers

Scam victims seeking redress currently face a significant information barrier and the SPF will make that barrier impossible to pass. Consumers are not empowered to find out if a business had objectively received 'actionable scam intelligence' on reasonable grounds or taken reasonable steps thereafter. Yet the consumer's entitlement to redress depends on proving these grounds.

Even if the sector Codes are more specific with respect to the expectations put on SPF entities, consumers are not likely to be able to understand this level of nuance or the interplay between the SPF principles and the Codes. The regime is complex, and obtaining and interpreting information to assess compliance will be even more complex.

[23] See: https://consumeraction.org.au/the-telco-code-has-run-its-course-and-failed-to-deliver-acma-must-explore-other-options-to-protect-consumers/
[24] See: https://insurancebrokerscode.com.au/ibccc-publishes-its-2023-annual-data-report/
[25] See: https://bankingcode.org.au/resources/bccc-report-compliance-with-the-banking-code-of-practice-july-to-december-2023/

Under the SPF, the consumer will not be required to prove breaches of obligations at the time they lodge their complaint, but rather at the time the scam happened, which is often sometime later. SPF entities will not publish all of their fraud prevention information – just like banks don't now – and this makes a consumer's task of proving their right to compensation even less plausible.

Imagine a consumer trying to obtain transparent information from Meta or Google. Even law enforcement find it extremely difficult to obtain information from these organisations to assist with their investigations. Similarly, international attempts to make the digital world safer have been unable to overcome end-to-end encryption.[26]

The information asymmetry does not only impact consumers. It is hard to see how one business – for example, the customer's bank – could determine its own liability for a scam under the SPF without understanding the liability of other banks, telcos and digital platforms.

David's story

David Sweeney's parents lost $1,000,000 to a scam in 2016, as reported in the ABC[27] recently. David advocated on behalf of his parents for years, but was repeatedly told that the bank could not have known that the transactions were the result of a scam, and no money was recoverable.

David lodged a Freedom of Information request to ASIC and in 2020 discovered that ASIC had put his parents' bank on notice of the investment scam months before their money was stolen.

After uncovering these documents, we understand that David's parents were swiftly subsequently reimbursed for most of their losses, five years later.

Ishan's* story – Financial Rights Legal Centre (S305251/ S305548)

Less than a year ago, Ishan received a spoofed text message on the same chain as his legitimate bank messages, providing a verification code and asking him to contact a number if he had not requested a verification code. As Ishan had not requested a code, he rang the number and the person who answered identified him in accordance with the bank's usual procedures. The person told Ishan two devices were attempting to access his account, and requested Ishan provide One Time Passcodes (OTP) to remove and block the unauthorised devices. Ishan did this, and the scammer used these codes to block his access to the account, link a new device, and transfer almost $50,000 from Ishan's account into another account with the same bank (then quickly out and overseas thereafter).

In response to a "suspicious activity alert" email from his bank after the transfers had taken place, Ishan rang his bank's call centre, and the bank identified Ishan was the victim of a scam. It was unable to recover any of his money. In refusing Ishan's request for compensation, the bank relied on various warning messages it had sent to Ishan, including generic broadcast SMS and emails about scam risk generally, as well as the warnings which accompanied the OTPs when Ishan generated them in the bank app and then unwittingly provided to the scammer. While Ishan acknowledged he may have received the generic communications, he denied having received the transaction-specific warnings; further, he said that the "warning" not to share OTPs with bank staff was inconsistent with previous practice by the bank, where this was routine.

During the course of Ishan's AFCA complaint, a significant amount of additional information was disclosed by the bank about its internal processes while the scam was taking place, including that no OTP was required when the scammer changed Ishan's online account password, that the bank's records were inconsistent as to whether an

[26] See: https://www.theguardian.com/technology/2023/mar/09/whatsapp-end-to-end-encryption-online-safety-bill
[27] See: https://www.abc.net.au/news/2024-09-16/government-scam-crackdown-leaves-banks-happy/104349596

OTP was or was not required to set up the new payee (the scammer), and that the bank identified the transaction as a potential scam and suspended both his and the receiving account, but did not inform Ishan other than to send a fairly bland email requesting he contact the bank. Whether these matters will impact the outcome in Ishan's case is unknown, as the matter is still before AFCA.

*Not his real name

SPF IDR must give consumers confidence and certainty and set strict timeframe limit on businesses

Unless the SPF sets minimum standards for all IDR processes to be fair and significantly streamlined for consumers, with strict time limits for businesses to provide fair redress or escalate to EDR, we cannot see how customers will have confidence in the IDR process or benefit from a good outcome, as illustrated by the Journey Map at Appendix A.

The SPF contemplates IDR response timeframes to be set out in the sector Codes. As it would make sense for all IDR timeframes to be standardised to be consistently applied across all SPF sectors, there is no reason why they cannot be specified in the Bill now. The UK has adopted a consumer-focused response time-frame model, where after a scam victim has initiated contact of a scam loss, banks are required to provide reimbursement within 5 days[28].

In Australia, the financial services framework requires responses within 30 days, extended to 45 for complex cases, and 21 days for financial hardship matters.[29] The ePayments Code requires financial institutions to investigate complaints and resolve them usually within 21 days. The current IDR timeframes in financial services are too long to apply to scam matters, including those that apply to the ePayments Code. Regardless which SPF entity an IDR complaint is lodged with, an IDR final decision before a matter is eligible to be escalated to AFCA should be no longer than 10-20 days in total. As per the policy intent in the UK, timeframes for scams IDR complaints need to be as short as possible, to minimise crippling financial and emotional harm, incentivise a response by businesses and provide certainty to scam victims. In addition, consumers must be clearly advised of their IDR options on first contact with an SPF entity about a scam (and the risk of delays if they do not initiate IDR) and it should *not* be the consumer's responsibility to contact the right SPF entity or add other parties to a complaint. These measures should be stated under a 'no wrong door IDR principle' that should be incorporated in the SPF Bill.

Recommendation

The SPF must include a consumer-focused standardised IDR timeframe across all SPF sectors no longer than 10-20 days, under a 'no wrong door IDR principle' incorporated in the SPF Bill.

Poor industry conduct toward consumers and power imbalance will carry over to the SPF

Scam victims are regularly treated poorly when they try to make a complaint. This includes being blamed for the scam, having to repeat their story after being transferred to different complaint departments of a bank, not being provided with information about AFCA, and not being provided with sufficient support to financially recover from a scam. Victims often tell us they feel they have been treated worse by their own bank than the scammer.

The EM at paragraph 1.197 states IDR is intended to encourage early resolutions. In practice, we see early resolutions offered at IDR are frequently low ball 'goodwill' payments. They often fall far short of what AFCA eventually determines the financial firm's liability to be. There is currently no industry standard for these amounts being offered, let alone any measures to ensure they are fair. We regularly see standard and unreasonable goodwill

[28] See: https://www.psr.org.uk/news-and-updates/latest-news/news/psr-confirms-new-requirements-for-app-fraud-reimbursement/
[29] RG 271.56, 271.67.

offers by banks, which are often closely aligned with standard AFCA complaint fees. There is nothing in the SPF to suggest this practice will change. Given the complexity of the proposed system and lack of consumer protections, most scam victims will accept these payments as they do now.

Vivian's* story – Consumer Action Law Centre

Consumer Action is assisting Vivian through an interpreter, who reached out after her life savings were stolen by scammers from her 2 bank accounts held with 2 of the top 4 major banks, totalling approx. $50,000, with each happening in short succession.

Vivian is a migrant and single mother relying on Centrelink income, who speaks very little English, with negligible understanding of technology, and suffers from significant mental health trauma due to her experiences before migrating to Australia. The scams have placed her in significant financial hardship and she is currently struggling with utility bills and educations debts. She is seeing a psychologist due to the significant mental and emotional impacts since being scammed.

All her savings were stolen after the scammers called her about an investment opportunity and manipulated her into downloading remote access software that she had never heard of on to her computer. They already knew a lot of her personal details and where very convincing to her as they spoke her native language. She states at no point did she provide any of her banking details, but the scammers were still able to access her internet banking, add new payees linked to obviously suspicious email addresses, and increase her low transaction limit significantly to make multiple large, completely out of character transactions over a number of consecutive days. There is evidence that a brief warning message was sent to her by the bank notifying her of possible fraud for the first payment, but in hindsight, Vivian states it was not a message that she would have properly noticed or understood if she did. Despite Vivian not responding to the warning, the bank allowed all the following transactions to proceed.

On each occasion after reaching out to both banks for assistance, despite her obvious vulnerabilities and language difficulties, neither bank offered or provided interpreters. On one occasion she desperately visited the bank branch and was told to call the bank's fraud phone hotline and again not provided an interpreter.

Only one bank has provided some vague documents to date in relation to the scam, but the poor treatment and non-assistance she has received by both banks since she has been scammed has added to her enormous and continued distress.

Both banks have offered only a very small fraction of her losses on a 'goodwill' basis but have denied any liability. Vivian has not accepted these and would like the bank to explain why their security systems did not flag and stop the transactions and what measures they will take to improve their security systems to prevent similar incidents from happening to other customers in the future.

*Not her real name

B. External Dispute Resolution

Single door EDR though AFCA is good – but still an impossible burden consumers

We welcome the proposal that consumers will have a single door EDR option through AFCA. It is highly likely scam victims will be unassisted, unsatisfied and out of pocket at IDR. Although EM paragraph 1.203 states EDR is intended to provide a pathway for where a SPF entity has not complied with their SPF obligations, like in IDR, we expect it will be extremely difficult for a scam victim to evidence their claim to redress at EDR, particularly as the dispute will expand out to multiple parties.

As AFCA stated in its decision of HSBC determination 12-00-1016692, a case only involving a single bank, but where the complainant was forced to engage a lawyer, incurring total costs of $8,442: "The arguments in this complaint have been extremely technical and nuanced and have required a thorough analysis of case law, knowledge of an industry code, the principles of statutory interpretation and substantive legal submission by the bank". AFCA also noted the "adversarial position" taken by the bank, awarding an additional $1,000 for non-financial loss compensation for the bank's failure to provide the complainant with the relevant requested information and meet the standards in the Banking Code following the complainant's notification of the disputed transaction.

We foresee AFCA having to work through many thousands, if not tens of thousands of scam cases it will likely receive each year. AFCA complaints are already at record highs, with a significant jump in complaints about scam-related issues, increasing 81% from last year to 10,951 in 2024.[30] Scam disputes at AFCA under the SPF will be significantly more complex than the typical complaint it handles today. AFCA itself has pointed to struggling to meet demand of less than 1,000 scam cases per month – likely a relatively small scams caseload compared to what will result from the SPF[31] –potentially tens of thousands of multi-party scam cases each year.

Apportionment unworkable case-by-case at EDR

Under the SPF as drafted, apportionment may also prove unworkable for AFCA. Based on our experience representing people in AFCA, with disputes involving more than one SPF entity, some of the issues we foresee AFCA having difficulties determining include:

- Liability and apportionment when some SPF entities have settled their claims at IDR;
- Liability and apportionment when evidence has not been given to AFCA because a claim has settled;
- How to deal with settled claims when AFCA may not be aware of some settled claims due to privacy;
- How to deal with multiple breaches of the SPF obligations versus one;
- How to deal with liability and apportionment when some SPF entities do not engage, including those denying liability and haven't had an opportunity to engage at IDR;
- Arranging multiple conciliations with various parties, or rescheduling due to the above;
- How to deal with causation and remoteness for each SPF, which would become more complicated with more than one scam being involved;

[30] Available at: https://consumeraction.org.au/afca-scam-complaints-off-the-charts-while-banks-fail-to-reimburse-customers/
[31] See: https://www.afca.org.au/news/media-releases/complaints-to-afca-top-100000-a-year-for-first-time

- How to deal with disputes between regulated entities; and
- How to deal with apportionment of compensation, including for non-financial loss and objections by SPF entities.

Apportioning liability is likely to always be left to AFCA, as it is highly likely businesses will not allow their liability to be determined by another business without legislative principles for apportionment set out in the SPF Bill. AFCA could be assisted with this task and many others, including with respect to information flow and identification and collaboration of cross industry systemic issues, if the Bill establish a relationship between AFCA and the TIO for efficiencies and to harness the years of specialist expertise and valuable goodwill that the TIO has fostered with the telecommunications industry over many years.

Furthermore, there remains the question about the extent that AFCA will be able to interrogate SPF entity claims that they met all their requirements. In our experience, AFCA does not always ask financial firms to back their statements and unevidenced assertions, and if it does occur, such evidence is not provided to complainants.

The EDR process must incentivise settlement at IDR

Under the SPF, businesses should be incentivised to assist consumers at IDR. Without such incentive, consumers are unfairly disadvantaged due to delay and scare tactics, complaint fatigue, power imbalances, information asymmetries and general low awareness of EDR options[32], particularly with consumer experiencing vulnerability. We know that AFCA fees alone are insufficient to incentivise resolution at IDR. This is evidenced by high numbers of claims rejected and years-long dispute resolution delays in the insurance industry.[33] A fairer system that increases access to justice could include the requirement that SPF entities *automatically* escalate scam complaints to EDR without the customer needing to apply, if a scam matter has not been resolved to the customer's satisfaction within a reasonable set time frame at IDR.

Similarly, there should be consequences for businesses who regularly default to EDR. Under the SPF, AFCA should be able to impose extra fees and increase levies on SPF entities who are found to have engaged in poor conduct or who regularly leave scam victims to turn to EDR (in addition to systemic reviews AFCA already undertakes).

We are equally concerned that under the SPF, compensation, even at EDR, would be unavailable for debt and interest incurred under a credit contract due to a scam. While there is a moral case that such money should be 'reimbursed' or reversed on the credit account, scam victims are often not entitled to compensation, despite the major financial hardship they have been put in due to the scam.

For these reasons, AFCA should be empowered to require banks to automatically halt interest being charged on disputed scam transactions and impose debt waiver determinations on credit funds that have been lost to a scammer, regardless of an AFCA finding of no liability on behalf of SPF entities. This should especially be considered for a complainant experiencing vulnerability or disadvantage.

Finally, although we do not consider it the intent of Government, we oppose any fees that may be imposed on consumers at AFCA if s58DC (2)(f) of the Bill would permit this. Similarly, s58DC(2)(c) of the Bill contemplates appeals to the Federal Court. Currently AFCA can only be appealed on very limited grounds by consumers. We would oppose a broad appeal power that undermines the purpose of EDR. Under no circumstance should SPF entities be permitted to commence appeals to the Federal Court against AFCA determination in favour of scam victims.

[32] See: https://www.tio.com.au/reports/barriers-effective-dispute-resolution-telco-industry-consumer-policy-research-centre-report
[33] See:https://insurancecode.org.au/app/uploads/2023/07/CGC-Thematic-Inquiry-into-Making-Better-Claims-Decisions.pdf; https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-221mr-asic-review-finds-insurers-can-and-should-improve-claims-handling/

Kylie's story* - CCLSWA

Kylie* was a victim of an investment scam where she lost approximately $55,000. The scam involved her investing in cryptocurrency and transferring money from her bank account directly to the scammers. The scammers also helped Kylie take out a loan to fund the fake investment. The scammers were sophisticated and built trust with Kylie. Kylie trusted the scammers to the point that she allowed them to use remote access software to apply for a loan that was larger than she wanted. Once the loan was approved, Kylie felt that she had to proceed with the "investment" in order to pay back the loan.

Kylie first transferred $2,000 to a cryptocurrency trading platform and received a payment of $30.19 which made her believe she was dealing with a legitimate company. The bank then called Kylie to warn she may be involved in a scam. Kylie told the bank it was not a scam and the bank later emailed her information about scams including the ACCC Little Black Book of Scams. Kylie had been told by the scammers that banks were clamping down on cryptocurrency trading, so she did not believe she was being scammed.

Kylie then transferred $20,000 to the scammers. The bank again warned her that it may be a scam, and placed a hold on a transfer of $19,500 that Kylie was attempting to make to the scammers the next day. The bank asked for information about the transfers and Kylie continue to tell the bank she was not being scammed as she trusted the scammers. Further, the scammers had played on public dissatisfaction with banks in Australia to build distrust between Kylie and her banks. The scammers told her things likes the banks were making record profits in a cost of living crisis but they want to keep your money rather than let you invest in cryptocurrency.

As the bank blocked Kylie's transfers, Kylie then withdrew cash and deposited the cash in a cryptocurrency ATM.

Kylie also transferred around $13,000 from one bank to a different bank as the scammers told her a certain bank would not block transactions. Kylie then transferred around $14,000 from this other bank account (in which the scammers had also sent around $1,000 to in an attempt to show the investment was legitimate) to the scammers.

When Kylie became aware she had been scammed, she reported the matter to the bank who were unsuccessful in recovering the funds. Further, the bank's position was that as they had warned Kylie of risks and that she may have been involved in a scam, they were not liable for the scam.

In this regard, Kylie asked the bank if she was being scammed at a certain point but as they did not provide her with a definitive answer, she continued dealing with the scammers.

Kylie's story is indicative of the sophistication of scammers and how they can build trust (and sow distrust with banks) to the point that any warnings a bank provides can be insufficient to dissuade a customer from proceeding with scam transactions. It may be that if banks had more responsibility for scam transactions, they would provide stronger warnings and provide greater scrutiny.

*Not her real name

Kathryn's* story - WEstjustice

Kathryn came to WEstjustice after she was scammed via SMS. The scam which affected her was a message purporting to be from Netflix and advising her that she was owed a refund after being overcharged for the service. Kathryn was from a low socio-economic background and because of past complex life events she can often be cognitively overwhelmed. She had indeed cancelled Netflix a number of months earlier to manage her household budget and was therefore a ready target for the messaging. Kathryn was asked to provide her credit account details to the malicious link and ended up with a debt to the maximum limit of her card of $5,000. At the time of the scam she had only $500 owing on the card.

Kathryn's bank was adamant that the matter was a scam and she was liable for the transactions. IDR negotiation on Kathryn's behalf resulted in her debt being halved. Kathryn decided she did not want to continue to fight the matter at AFCA.

*Not her real name

Recommendation

The EDR process must incentivise fair settlement by businesses at IDR.

Recommendation

Disputes must be automatically escalated to AFCA by businesses if a consumer is dissatisfied with an IDR resolution.

Recommendation

AFCA should be able to impose extra fees and increase levies on SPF entities who are found to have engaged in poor conduct or who regularly leave scam victims to turn to EDR.

Recommendation

AFCA should be empowered to require banks to automatically halt interest being charged on disputed scam transactions and impose debt waiver determinations on credit funds that have been lost to a scammer.

Transparent information sharing, including via AFCX

Information sharing must not be restricted by privacy arguments

Arguments about privacy are preventing scam victims, EDR bodies and regulators from accessing the information they need to combat scams, including concerning mule and fraudulent accounts. If privacy laws prevent a consumer from accessing information to prove their case under the SPF, this is yet another fundamental reason why the SPF needs to include a presumption of reimbursement.

Confidentiality and non-disclosure agreements

Another issue that may impede transparent information flow and disputes processes include scam victims being unable or extremely hesitant to disclose key information, including at EDR, if they were previously told it might be in breach of a settlement agreement agreed at IDR with an SPF entity. For this reason, confidentiality and non-disparagement clauses and all forms of non-disclosure agreements (NDAs) should be prohibited under the SPF. We have seen prolific use by banks of NDAs in scams cases at all stages of the dispute resolution process including before and after IDR and EDR. The use of NDAs by banks in relation to some of our clients' scam matters has also limited our ability to share relevant case studies with Government as part of this consultation.

AFCA must be empowered to obtain all relevant information via the AFCX

As identified in our previous submission to the Treasury scams consultation paper,[34] in the majority of cases, scam victims are unsuccessful at AFCA. They often don't have access to information to assess whether or not the bank met its existing obligations regarding scams. Part of this problem arises because IDR and EDR require a business to produce information contrary to their own interest. This puts scam victims on an unlevelled playing field from the start, and it is often unclear to the scam victim if the bank is providing AFCA all relevant information to ensure a fair outcome, such as in AFCA determination 12-00-1016692, or AFCA determination 998769 which specifically pointed to bank's failure "to provide key information to assist AFCA with its investigation", after repeated requests.

Although we believe it may take to the end of the decade to develop and work as it needs to, a streamlined information sharing system of actionable scam intelligence by regulators that is easily accessible by consumers (if they need to prove their case), AFCA and businesses in a timely way, must be facilitated by the AFCX. Transparent and easily accessible information must:

- ensure all relevant information is shared with regulators in the first instance (and subsequently to consumers, AFCA and businesses) - this information may need to be de-identified but privacy arguments should not prevent the information sharing; and
- not drown consumers in unintelligible and overwhelming volumes of data logs and documents.

AFCA would also need timely access to all relevant internal policies and operations of SPF entities in the first instance.

Recommendation

Actionable scams intelligence must be easily accessible via the Australian Financial Crimes Exchange (AFCX) in a way that reasonably minimises information asymmetries for the consumer.

[34] See: https://consumeraction.org.au/scams-mandatory-industry-codes-consultation-paper/ - A Consumer Action Law Centre examination and analysis of 50 AFCA final determinations between 18 September 2023 to 12 December 2023 in relation to scams (or potentially fraud), found that consumers were successful in only 4 matters (approx. 8% of determinations).

Recommendation

Actionable scams intelligence must not be restricted by privacy arguments.

Recommendation

The SPF Bill or Codes should prohibit confidentiality and non-disparagement clauses and all forms of non-disclosure agreements (NDAs).

Resource implications for community lawyers and financial counsellors

The nature of the scam epidemic in Australia leads us to conclude that there will be an exceptionally high number of cases brought to IDR and EDR, with multiple businesses involved each time. Financial Rights Legal Centre have provided the following costing for legal services they provide for scam matter as a guide and how they would significantly increase under the SPF.

"Since 1 January 2023 Financial Rights Legal Centre has spent an average of $28,000 per month in labour costs (excluding administration and overhead costs), dedicating approximately 94 hours on average each month to provide crucial information, advice, task support and representation services to clients who have been scammed. These costs fluctuate significantly from month to month and have reached as high as $69,000 a month with up to 240 hours of dedicated support.

These costs are however based on the current delivery of client support, which is predominantly advice and information rather than representation. This is due to the limited rights in place to support the representation of clients to obtain compensation or reimbursement of monies lost through scams. If there were more rights in place – for instance, under the proposed SPF – these costs would increase significantly as the service would likely provide increased representation services. This could mean a 10x or more increase in costs, potentially reaching up to $690,000 per month given the resources required to manage casework through IDR and EDR regimes."

"Anecdotally we know that there are far more scam victims out there who don't even bother reporting it (either from shame or lack of belief in the system). This cohort may well start reporting their cases when the legislation comes in, which will only further strain the proposed IDR/EDR process" - Claude, Financial Counsellor Consumer Action Law Centre.

4. Other limitations with a 'prevention only' focus

- Nearly every scam involves a mule or fraudulent account
- Warnings are not enough
- Scams sophistication and artificial intelligence – SPF places a high bar on consumer responsibility

Prevention, warnings and education for consumers will never be enough to address the scams epidemic. The SPF needs to recognise the reality facing consumers, particularly the complexities they have no control over and growing threats from scams. Vulnerable consumers stand to particularly lose out and remain exposed to scams and unassisted under the proposed framework.

The SPF relies heavily on consumers to remain hypervigilant at every turn, prosecute complex arguments through dispute resolution, and very likely continue to shoulder the overwhelming majority of scam losses.

Nearly every scam involves a mule or fraudulent account

Receiving banks in the UK are responsible for 50% of scam losses that occur on their platforms. In contrast, the SPF does not provide a clear indication that Australian banks will be held equally liable as a default for allowing the proceeds of scams to flow through their systems. Obligations to act on 'actionable scam intelligence' will, in practice, impose obligations after a scam report has been received – it does not incentivise banks to prevent mule or fraudulent accounts in the first place.

In our experience assisting scam victims, money is always funnelled through an account that has been compromised. This indicates systemic failures by receiving banks almost certainly not meeting their Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations. We are concerned that the EM at paragraph 1.78 contemplates the SPF rules excluding conduct regulated under AML/CTF legislation. We think this is a missed opportunity to actively tackle the role of mule and fraudulent accounts involved in scams, which is crucial to stemming losses.

We appreciate that the Australian Banking Association and Customer Owned Banking Association's voluntary Scams Safe Accord requires additional identity verification requirements for new accounts including biometric checks.[35] While banks claim to be employing technology to tackle mule accounts,[36] it has not had a measurable impact on scam losses. Banks have been on notice of the scale of the problem for a very long time.[37]

The SPF must set the highest possible bar and place further obligations on banks to ensure mule accounts are not operated. Incentives could include greater penalties or compensation at EDR for banks hosting mule accounts. Obligations should also include stronger monitoring requirements including additional checks on inactive or bank accounts displaying a range of unusual activities.

Recommendation

The SPF must set stronger measures to stop mule and fraudulent accounts being used to perpetrate scams, and introduce meaningful penalties for banks that allow the opening and operation of scam mule accounts on their platforms.

[35] See: https://www.ausbanking.org.au/scam-safe-accord/
[36] See: https://www.anz.com.au/newsroom/media/2023/august/anz-to-implement-mule-account-detection-capabilities-in-continue/
[37] See: https://www.ausbanking.org.au/wp-content/uploads/2019/04/ABA-111084-v1-Fact_Sheet___Money_Mules_Explained.pdf

Warnings are not enough

The focus on warnings as a scam prevention measure is out of touch with the reality of human behaviour. In our casework we regularly see that standardised and even quite specific warnings fail to disrupt social engineering tactics utilised by scammers. The past few years has made it clear that scams cut across language, literacy, levels of education or cultural backgrounds and that we cannot warn or educate our way out of the scam epidemic.

The SPF Bill at s58BK (2)(a) only requires SPF entities to identify or provide a warning to consumers who are at a higher risk of being targeted by a scam. This is a very low standard of care. Instead, the SPF needs to make it clear that SPF entities, especially banks, need to do more than provide standardised warnings to high risk or vulnerable consumers. They should provide warnings that are tested, and that work.

The SPF also needs to do more to clarify when a warning will be insufficient, and banks should proactively prevent scams, rather than issue a generic warning. Currently, the banks tell us they have no obligation to monitor account holders' transactions for signs of fraud. Not only is this out of step with community expectations, it is also far below their existing capability to do so. In our casework, we frequently see scams where obvious red flags are raised that indicate the customer is being scammed, for example:

- Spending tens of thousands of dollars on a credit card that hasn't incurred more than a few hundred dollars in years; and
- Issuing several multifactor authentication codes, resulting in a new mobile banking app authorised, transfer limit increased and high value transactions immediately made.

It is well within the resources and practices of banks to develop algorithms to monitor customer transactions. These algorithms should be used to identify suspected indicators of scams and make further inquiries when red flags are raised. Limiting the obligations on banks to just warnings in the SPF could translate to lower requirements and standards being implemented in the sector Codes.

2023-2024 HSBC Bank impersonation scam

Consumer Action Law Centre has been in contact and provided assistance to some of the more than 60 HSBC scam victims, many who lost their life savings to this scam totalling more than $6.3 million – a figure reported by the ACCC in March 2024. Victims have told us the scams were seamlessly permitted on the bank's platforms, after new phone numbers were registered to their accounts, quickly followed by an increase in their transaction limits, before their accounts were drained at $50,000 at a time. Actions that if looked at in isolation may not arouse suspicion, but should have been obvious to HSBC that more needed to be done to protect its customers from the very first report. In some of these scam cases bank accounts were accessed both in Finland and Australia in quick succession which would have been impossible to action by the customer on their own.[38]

These customers had no choice but to escalate their matters to AFCA, after they were told the bank was not at fault and received little assistance from HSBC. Meanwhile, HSBC in the UK are reimbursing 76% of scam losses to customers.[39]

[38] See: https://www.theage.com.au/national/not-a-single-care-victims-of-hsbc-fraud-say-bank-could-have-stopped-the-scammers-20240716-p5ju22.html
[39] UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

Samirah's* story (Romance scam) – Consumer Action Law Centre

Samirah called the National Debt Helpline in early 2024 for help. She speaks a language other than English at home and works full time in a retail store. She was struggling to repay two personal loans and meet her living expenses.

When our financial counsellor spoke to Samirah, she explained that she had been groomed by a person she met on a dating app to invest tens of thousands of dollars over the Christmas and New Years holidays. Initially, Samirah had believed him when he said he was interested in a relationship, and gave him her number to message her through WhatsApp. She told him that she was struggling to pay her rent, which would increase soon, and he told her he could show her how to make money through trading cryptocurrency. He helped her to set up accounts with different crypto currency, and at first she transferred just $200. The scammer showed Samirah investment updates that included major profits from her crypto currency.

The scammer encouraged Samirah to send more money, and they spoke about what she would spend the proceeds on. The scammer regularly told Samirah that he didn't want her to worry about money or have to work when they would be together. He texted her to drive safely on her way home from work.

When Samirah went to transfer substantial amounts from her bank accounts to the crypto exchange, one of the banks displayed a warning that she should consider whether this was a scam and not to proceed. The warning also said that her bank might not be able to recover her money if she did proceed. Samirah spoke to the scammer about the warning. He said that they always displayed those warnings and not to worry.

Samirah had run through her savings when she was told her cryptocurrency account would be closed unless she sent thousands of dollars more. She started applying for loans. Samirah was declined by several lenders but eventually was successful with two non-bank lenders and was approved for loans totalling $20,000. One of the non-bank lenders took security over her car. When Samirah asked her brother for money, he told her it was a scam.

The cryptocurrency platform told Samirah that her account with them was real, but the website address she'd sent the crypto to from their platform wasn't legitimate. Samirah faces the prospect of raising disputes with both of her banks, as well as the lenders, to try to recover some of her money and obtain financial hardship assistance.

*Not her real name

Kheti's* story – Consumer Action Law Centre

Kheti is in Australia as an international student. While she is on a bridging visa, she is unable to work. Kheti responded to a post on a Facebook group for cash in hand jobs. The poster quickly put her in touch with another person through WhatsApp and Telegram, who told her she could earn money by writing reviews for products online. To write the reviews, she had to send money through cryptocurrency – she transferred from her bank account to a money transfer platform, and then to a crypto platform. Her bank sent a message to her to see if she authorised the transaction, however as Kheti received a number of automated pop-ups or messages through the apps from her bank and the money transfer platform, Kheti just clicked through them. The money transfer platform also displayed a specific warning that the transfer could be a scam.

Although Kheti was suspicious, she sent $75 and received $250 on the first day, which made her think it was trustworthy. The scammers asked Kheti to pay more and more money over the next few days. Kheti had transferred $4,300 before she realised it was a scam, and reported it to her local police, her bank and the payment platform. She called Consumer Action for assistance in mid 2024.

Kheti says that her bank wasn't willing to assist her and told her the money was gone. She raised a case with the money transfer platform, who are still looking into it several weeks later but said it was unlikely they would be able to retrieve any of the money. Kheti needed the $4,300 to pay her tuition.

*Not her real name

Recommendation

Strengthen s58BK 2(a) to require businesses to do more than only identify and provide warnings to consumers at a higher risk of scams.

Recommendation

Strengthen s58BD to require banks to proactively monitor transactions – and provide more detailed actions and examples in this respect in the EM.

Scams sophistication and artificial intelligence – SPF places a high bar on consumer responsibility

Advances in technology and the increasing sophistication[40] of scams means that people are simply never in the best position to address that risk. No one can have the confidence that they will be vigilant enough to be immune from being scammed in light of widespread personal data breaches. The OAIC recorded 527 data breaches from January to June 2024 alone, which included 12.9m Australians affected by the MediSecure data breach, the second breach affecting over 10 million Australians in just the last few years.[41]

We receive unique insights from our frontline services – not only as to the level of precision in complex and elaborate scams, but also the immense shame experienced by a wide range of people who would never have believed that they could fall victim to a scam. Many victims of scams typically have no idea how the scammer was able to obtain all the details needed to access and drain their bank accounts (e.g. AFCA determination 998769).

[40] See: https://www.accc.gov.au/media-release/its-a-scam-celebrities-are-not-getting-rich-from-online-investment-trading-platforms#:~:text=%E2%80%9CScammers%20are%20creating%20fake%20news,fact%20it%20is%20a%20scam.%E2%80%9D

[41] See: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024

AFCA recently held that it is difficult, if not impossible, for a consumer to readily identify when they are legitimately dealing with their bank, or when a third-party has intercepted the bank's communications channels.[42] This reflects the reality that people are navigating every day.

Scammer often create a sense of urgency that the consumer needs to take action, and while anyone can be targeted and deceived, consumers experiencing vulnerability and disadvantage will remain particularly susceptible.

Nadia's* story – Consumer Action Law Centre

Several weeks ago on a Sunday, Nadia received texts from her bank saying that her mobile number had been changed, and had received several multi-factor authentication codes. She checked her accounts and discovered money had been withdrawn from her accounts including the home loan she has with her husband. There were several transactions at a supermarket in another state. Nadia called her bank and after waiting on the phone for hour, they told her that they'd locked her account and to come into a branch in the morning.

When Nadia attended the branch they told her the transactions had cleared, despite her reporting them as fraudulent when they were still pending. The staff helped her to ring the same number she had called the day before and she waited another 40 minutes to speak to someone. Some of the charges were classified as credit card fraud and some as digital fraud. This meant that multiple teams had to investigate. They told her that another phone number had been added to her account. That number was removed, and Nadia changed her passwords. She withdrew a few hundred dollars in cash and then her accounts were locked.

Nadia went home and had her phone and computers cleaned and reset, on the advice of the bank.

After Nadia and her husband received their next fortnightly pay, her phone company texted her to say that her email had been changed. Nadia had several phones for her family, which all stopped working and displayed 'SOS only'.

When she called the phone company they told her to come into the store. The store assistant told her that the email that had been added to her phone account was nearly the same as hers – just a few extra characters. She had that email removed and replaced with her real email.

Nadia then attended the bank branch again, where they told her that she had opened a new account the day before, which she hadn't done. She discovered new fraudulent charges which she reported. The bank told her the account would be blocked again until they had their phones and computers reset again. Nadia and her husband did that and changed all their passwords.

Nadia has access to her employer's banks accounts and was worried that the scammers would steal that money too, so she told her boss to remove her access and keep a close eye on the accounts.

More emails came from Nadia's bank on another Sunday, this time saying that she had created a new PayID. When she called her bank, she says they told her that she shouldn't worry as her account is blocked, but to attend a branch – and none were open until Monday. The branch staff told her that she had applied for two business loans and there were several thousand dollars in new charges she hadn't authorised. The bank said that the applications and transactions had gone through because they came from a phone, although they told her it was a different model of iPhone than the one she has and her phone number must have been ported.

When Nadia asked her phone company how that had happened, they said that someone had called pretending to be her, saying that she had been in a major card accident and needed a new sim card posted to her straight away.

[42] AFCA ref 12 00 1016692

The store wouldn't tell Nadia the address they'd posted the new sim card to. Nadia then asked the phone company to set up her with new numbers and changed her email address. She says that they didn't ask her for any identification until she told them she had to change the bank details associated with her account.

Nadia spoke to Consumer Action and lodged a complaint with the TIO and AFCA about the scam. She says that after lodging the complaint, the bank started to be more helpful, and contacted her proactively instead of making her wait on hold. Her bank has recovered most of the money that was stolen, with just a few thousand still under investigation.

Nadia says that she doesn't feel secure anymore after her experience. She says that she enters 'panic mode' when she receives a call from an unknown number. Nadia doesn't feel safe with her bank, but she can't change banks because of her joint mortgage. She constantly checks her banking apps to ensure that her money is safe. At times throughout this experience she and her husband had virtually no access to cash.

*Not her real name

5. Higher bar needed to protect and provide assistance to consumers experiencing vulnerability and disadvantage

- Scam victims impacted by vulnerability and disadvantage
- Experience of First Nations communities

Scam victims impacted by vulnerability and disadvantage

The SPF does not specifically establish obligations to identify and protect consumers experiencing vulnerability or disadvantage.

Section 58BK of the SPF Bill says that SPF entities should proactively identify consumers, but not on what basis. It may mean that receiving actionable scam intelligence will trigger an obligation to warn consumers that they may be at risk of a scam due to their susceptibility, being in a particular geographic area, the language they speak, or the banking product they hold. While these are all important and a desirable outcome of the SPF, an obligation to identify and protect consumers experiencing vulnerability and disadvantage from scams should be treated separately and with sufficient detail.Further detail could be set out in the Codes. This would not only recognise the disproportionate impact scams have on vulnerable consumers, but would hold businesses to a higher standard to mitigate harm on people experiencing these circumstances from scam and allow appropriate redress if a business has not met that standard.

There is an emerging body of research on the impact and harms of scams being experienced by people experiencing vulnerability and disadvantage. Monash University and CyberAbility recently published research on the psychological and social impacts of scams and the disproportionate impact on people with acquired brain injuries (ABI) and other disabilities. [43] The research found people with an ABI are 50% more likely to be scammed online and an average loss of $20,000.

The Banking Code of Practice requires subscribers to take extra care with customers experiencing vulnerability.[44] Despite banks already holding much information to determine this about their customers, the onus remains on the customer to establish that the bank was aware of their vulnerability (e.g. AFCA determination 996924).

The SPF has the opportunity and needs to go beyond existing, virtually self-regulated[45], industry practice to ensure that all consumers experiencing vulnerability and disadvantage are adequately protected and that businesses are held to community expectations.

The SPF should include an overarching goal to reduce the incidence and harm from scams on people experiencing vulnerability and disadvantage. It should direct the sector Codes to require additional steps from businesses to comply. The ACCC and the NASC[46] already report on cohorts that experience vulnerability, including First Nations peoples, people living with disabilities, culturally and linguistically diverse communities and the elderly. We know that consumers experiencing vulnerability and disadvantage are likely to be disproportionately impacted by scams and the SPF needs to reflect this reality.

[43] See: https://cyberability.org.au/support
[44] Chapter 14
[45] Available at: https://www.ausbanking.org.au/wp-content/uploads/2021/05/ABA-Family-Domestic-Violence-Industry-Guideline.pdf
[46] National Anit Scams Centre, ACCC. 'Targeting scams: Report of the National Anti-Scam Centre on scams activity 2023'. April 2024. Available at: https://www.nasc.gov.au/reports-and-publications/targeting-scams

Renate's* story - WEstjustice

During 2021, Westjustice assisted a large number of people from the Communities of Burma who had been victims of an app-based investment scam. These clients were especially at risk of being affected by scam transactions due to language and technological barriers which meant that they were vulnerable to being targeted. The app was in some cases downloaded from parties which would come under the scope of being Digital Platforms for the proposed framework.

A consistent theme among the clients, was that their banks had either not had warnings about making payments to a new payee, or those warnings that were present were not effective warnings. Additionally, when Renate first realised that she had been scammed she tried to call her bank but was told an interpreter could not be provided to help her make herself be understood.

Renate was assisted by Westjustice to get partial compensation, but this was after a lengthy AFCA process which went to final determination and compensation was awarded solely on the basis of arguable Banking Code breaches with respect to facilitating interpreter access. Despite only losing $4000.00, the impact on Renate's family included food and school fee stress, and the inability to repair her vehicle for transport. The matter took 18 months to resolve.

**Not her real name*

Experience of First Nations communities

The large onus placed on ordinary people under the proposed SPF is likely to exclude many First Nations people from seeking redress after they have been scammed - particularly those in remote communities where decades of underinvestment in communications infrastructure have left people digitally excluded. IDR and EDR involves constant access to communications which is a barrier for a lot of people in remote First Nations communities.

Consumer Action's 2024 report *Money Yarns, Stronger Futures* conducted research with First Nations consumers in Victoria to identify legal issues. [47] The report identified significant underreporting of scam losses experienced by First Nations people, which may be driven by feelings of shame, lack of trust in banks (including due to previous past poor experiences and treatment) and Government, not identifying a scam, or lack of knowledge of the reporting process or support services to escalate their scam matter. Six of the nine First Nations people that were interviewed *Money Yarns* mentioned they had been the victim of a scam, but only one person had reported this to a regulator.

One First Nations interviewee who had lost money to a scam told of us of her experience:

"I rang the bank soon after the money got taken out and they said I would have to call them back in regards to reimbursement. They said at first you have to get your phone cleaned, and while my phone was getting fixed they scammed me a second time. I ended up getting my phone reset again and I was waiting for the bank to reimburse me and they go you haven't asked us to reset or actually claim for it and I said I did (when I had) rung up. When I went into the bank they thought I was deaf, they were so rude.. they said oh she's only closing her account because she got scammed.. I heard every word."

[47] Consumer Action Law Centre and the Victorian Aboriginal Legal Service, July 2024. 'Money Yarns, Stronger Futures: The consumer, credit and debt issues of First Nations consumers in Victoria '. Available at: https://consumeraction.org.au/report-money-yarns-stronger-futures/

Tailored obligations for SPF entities towards First Nations consumers that could be addressed in the Bill could include, for example, the need to ensure culturally safe complaint avenues and assistance is provided for First Nations consumers who have been impacted by scams.

Key Recommendation

Introduce an overarching goal and provisions in the Bill that require businesses to do more to protect consumers experiencing vulnerability and disadvantage from scams. The EM should also provide examples of the higher bar placed on businesses to identify customers experiencing vulnerability, address their extra need, and protect them from scams.

6. Regulation and enforcement, the ePayments Code and other sectors

- Sector regulators
- Higher penalties needed - civil penalties, infringement notices and other penalty provisions
- ACCC review after 18 months
- ePayments Code - consumers must not be worse off
- Other sectors - superannuation, digital currency exchanges, digital marketplaces, non-ADI financial services, payment and money transfer platforms

Sector regulators

We welcome the proposal to have the ACCC as the SPF general regulator and digital platforms Code regulator.

Without a reimbursement model, the ACCC will need to be resourced substantially along with ASIC and the Australian Communications and Media Authority (ACMA) who are proposed to be the designated sector Code regulators to enforce the SPF, given that the proposed SPF dispute resolution will not incentivise compliance.

Higher penalties needed - civil penalties, infringement notices and other penalty provisions

Although welcomed, we are concerned the higher tier one penalties will rarely be applied, as they are set up to mainly target high level systemic and breaches of SPF principles, enforced by a single regulator across multiple sectors. In reality, breaches of the Codes are more likely to be enforced, but these attract much smaller penalties for similar conduct.

We can imagine cases where tier one penalties must also be accessible to regulators for Code breaches which are currently proposed to be covered by the significantly lower tier two penalties. Further clarity is required to determine whether regular or systemic non-compliance of a Code will be enough to attract tier one penalties. For the SPF to be taken seriously by businesses, the highest possible penalties should be at the disposal for sector regulators for all breaches of Code obligations.

Infringement notices, currently set at a maximum of $18,780, need to be significantly increased, at least for the larger SPF entities, if they are going to have any effect on the compliance practices of major banks, telcos and digital platforms. We also do not agree with infringement notices not being valid unless issued within 12 months of a contravention.

Section 58FJ of the Bill prohibits the issuing of multiple pecuniary penalties under two separate provisions for same SPF contravention. Further clarity and thought is required to ensure this provision will not limit stronger action for systemic breaches, or lead to multiple breaches of different SPF principles or Code provisions going unpunished.

Finally, we require clarity as to the treatment of contraventions of any non-civil penalty obligations that may be included in the Codes. We do not support any voluntary provisions in either the SPF or Codes that would in any way limit the liability of businesses' obligations under the SPF.

Recommendation

Tier one penalties must be available for all Code breaches, or at least systemic Code breaches, and the penalty specified for infringement notices under s58FN must be significantly increased.

ACCC review after 18 months

We support the ACCC's overarching jurisdiction as the general regulator to monitor and supervise compliance with the SPF provisions and conduct thematic reviews. However, the SPF needs to set up a mechanism for the review of the SPF and sector Codes on a regular basis to ensure they will be effective on a number of different levels.

As the development of the new SPF is novel and untested, we recommend that the ACCC is empowered and funded to undertake a review of the regulatory regime 18 months after it commences. The review should focus on consumer outcomes, with a particular focus on the effect on and experiences off consumers experiencing vulnerability and disadvantage, which has not been well-documented to date.

The Government should ensure the ACCC has adequate data collection powers for this, particularly considering the regime may apply to other types of sectors in future.

Recommendation

The ACCC should be funded to undertake an independent review of the SPF after 18 months of its operation, with a focus on outcomes of consumers experiencing vulnerability and disadvantage.

ePayments Code - consumers must not be worse off

It is important that the consumer protection aspects of the ePayments Code are not compromised. The limited number of scam complaints that fall under the ePayments Code benefit from certain presumptions that put the onus on their bank to prove certain relevant facts.[48] We expect that banks will prefer scam complaints to be considered under the SPF rather the ePayments Code because it gives rise to sharing liability for scam losses between businesses, which the ePayments Code does not contemplate. If more consumers are pushed towards the SPF to seek redress, then the SPF should provide better rights and simpler processes to redress than under the ePayments Code.

The SPF could set up a regular showdown between consumers and businesses where scam victims will have to fight at IDR and EDR to get their money back to a greater extent than the current ePayments Code process, without the benefit of the existing presumption. AFCA has recently expanded on its interpretation of 'voluntary disclosure' under the ePayments Code. In a recent case it clarified that where the level of deception was so high, the complainant could not be held to have voluntarily disclosed their passcode.[49]

We fear that banks may reduce assessing cases for reimbursement under the ePayments Code, relying on actions taken under the SPF to prevent/detect/disrupt the "scam".

To avoid doubt, a provision should be included in the SPF Bill to make clear that the SPF, and the SPF Code for banks operates in addition to, and not in derogation of, the rights of a customer under the ePayments Code.

Recommendation

The SPF Bill to make clear that the SPF, and the SPF Banking Code is in addition to, and not in derogation of, the rights of a customer under the ePayments Code, who must also have an easier and streamlined pathway to redress than currently under the ePayments Code.

[48] E.g. ePayments Code clauses 10.4, 11.2 or 11.5.
[49] See: https://my.afca.org.au/searchpublisheddecisions/kb-article/?id=f9f8941f-7379-ef11-ac20-000d3a6acbb4

Other sectors - superannuation, digital currency exchanges, digital marketplaces, non-ADI financial services, payment and money transfer platforms

The EM contemplates the designation of the banking, telecommunications and digital platform sectors in the first instance under the current reforms. Scammers don't just contain themselves to these areas. An effective SPF will cause a significant uplift in protections across the banking sector, which is likely to result in scammers targeting other sectors that will remain highly exposed to scams.

We call for timely designation of other sectors to extend the SPF to superannuation, cryptocurrency, in addition to digital marketplaces, non-ADI financial services and insurers, payment and money transfer platforms.

In particular, we are disappointed that the initial remit of the SPF will not include online marketplaces, and particularly Facebook marketplace, despite the majority of Facebook seemingly being within the intended remit. It is no secret that Facebook marketplace is a platform with a serious scam problem.[50] Expanding the SPF to address existing hotbeds for scams should be a major priority going forward.

With $3.9 trillion dollars currently held in superannuation assets and an average member account balance of $165,000,[51] it is no surprise that scammers are already turning their eyes to the super system.[52] The moment there is an uplift in banking, telco, and digital platforms scam prevention, we expect that scammers will turn to superannuation in greater numbers – and the superannuation industry is not ready to respond. Greater and swifter regulatory intervention is required to coordinate and drastically uplift super fund responses to scam activity, which is why we are calling for the superannuation sector to be designated under the SPF within a year of the SPF receiving Royal Assent.

Non-bank credit providers and non-ADI payment platforms, including purchase payment facilities and money transfer services (e.g. Paypal, Wise and Western Union) are currently not intended to be covered under the SPF. This in unlike the UK, where the mandatory scams reimbursement model to commence in October 2024 covers a wide range of regulated 'non-directed' payment service providers (PSPs).[53] This includes non-bank 'payment firms' and FinTechs. We also understand that cryptocurrency platforms will be licensed under the AFSL regime in the near future[54] and suggest that designation under the SPF should swiftly follow.

Jill's* story – Consumer Action Law Centre

Jill's bank account was hacked by a scammer with a number of unauthorised transactions out of her account. She also found out that a fake Wise account was set up in her name and funds were transferred overseas. Jill says the bank did not help, blaming her for what happened and said it would take 45 day to review the matter. She made a report to police and lodged a complaint against Wise, who could not assist as they said it was a fraudulent account in her name.

Jill is a student who only just had commence working part time work and lost her entire saving of just under $5,000 to the scam. She is now behind on her share house rent and has no money to pay the gas bill in her name.

*Not her real name

[50] See: https://www.abc.net.au/news/science/2024-03-01/facebook-marketplace-has-become-the-home-of-scammers/103521536

[51] See: https://www.ato.gov.au/about-ato/research-and-statistics/in-detail/taxation-statistics/taxation-statistics-2021-22/statistics/individuals-statistics

[52] See: https://superconsumers.com.au/wp-content/uploads/2024/03/SuperConsumersSubmissiononScams%E2%80%93MandatoryIndustryCodeconsultation.pdf

[53] UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. p.18. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/; Although they accounted for a significantly smaller amount of scam losses than the major banks, the PSR found that 2023 scams rates for non-directed firms in the top 20 list of receivers of scam funds were typically much higher than those of directed firms.

[54] See: ASIC: Crypto start-ups should hold financial services licences (afr.com)

With the passing of the Consumer Data Right (CDR) Action Initiation Bill, there is now a more pressing need to ensure that FinTech organisations and FinTech applications powered by the CDR (especially those involving payment/action initiation) will soon be subject to the same scam codes standards as banks, social media and telcos. Although the CDR and action initiation proposals have the potential to assist consumer make better use of their own data and promote competition between businesses, the rapidly evolving landscape where scammer are looking to exploit every loophole, requires the Government to ensure all consumer safety recommendation for the development of digital ID, scams laws, and in relation to the Privacy Act review are in place before CDR and action initial come online.

Recommendation

Future sectors, including superannuation, are designated within 8 months of Royal Assent. Government should commit to this timeframe by documenting it in the EM and parliamentary speeches.

7. Timing and designations – consumers being harmed can't afford to wait

Australians continue to lose their life savings and hundreds of millions are lost from our economy to scams every month. Industry has failed to step in and invest the level needed to protect their customers or repay them for failing to keep their money and information safe. **Government now needs to step in**. Against this background, the need **to urgently pass strong SPF laws – with some much-needed improvements** – cannot be overstated.

While Australia's SPF is estimated to come online as late as 2026-2027 or beyond, UK consumers will benefit from a mandatory bank reimbursement scam protection from October 2024. Unlike Australia, in the UK, confirmation of payee has been in place for years and progressively expanded since 2022 to provide the service to include approximately 400 additional firms.[55] In Singapore the mandatory SMS ID registry has resulted in a significant reduction in scam SMS messages.[56]

Meanwhile Australian banks will continue to reimburse their customers only 2-7 percent of scam losses that flow through their platforms and account for the majority of the $2.74b being lost to scams every year.

Until the Codes are brought into force and the SPF is up and running, consumers will remain unprotected without strong obligations on businesses to prevent and respond to scams. AFCA will continue to hear cases in a vacuum, and scam victims will continue to lose out. As illustrated by the consumer Journey Map, a presumption of reimbursement will be far simpler and easier to implement that the proposed SPF compensation model. This would also mean the SPF and sector Codes could be brought into force much earlier to start protecting all Australians from scams.

Suggested SPF implementation timetable:

End of 2024	Draft Codes for telcos, digital platforms, and banks are published for consultation
Upon Royal Assent of SPF Bill	Telco, digital platforms, and banking are designated by the Minister. SPF principles apply immediately.
8 months post Royal Assent (mid-2025)	Telco, digital platforms and banking Codes are introduced, designated sectors given 8 weeks to comply
8 months post Royal Assent	Future sectors designated, including superannuation and cryptocurrency exchanges
12 months post Royal Assent	Next round of Codes introduced, designated sectors given 8 weeks to comply
12 months post Royal Assent	EDR and apportionment of liability mechanism finalised and implemented
18 months post Royal Assent	Review of SPF framework

[55] UK Payment Systems Regulator. 'Authorised push payment (APP) scams performance report'. July 2024. p.25. Available at: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

[56] See: https://www.choice.com.au/consumers-and-data/protecting-your-data/data-privacy-and-safety/articles/bank-impersonation-scams

Recommendation

The new SPF laws should be implemented by mid-2025, with the sector Codes up and running within 8 months of Royal Assent of the SPF.

Recommendation

The Government to release drafts of the Codes for consultation before the end of 2024.

APPENDIX A – Hypothetical Consumer Journey Map

Consumer Journey under **SPF**

This is a hypothetical case study and journey map across **(1) the proposed SPF dispute resolution vs. (2) reimbursement framework**, with the information available to us, and based on our scams dispute resolution experience.

The SPF is high level, principles-based and leaves much of the detail of what dispute resolution will look like to be determined later. Despite this, we think it is important to map - even hypothetically - what the process could look like to ensure Government doesn't commit Consumers to a system containing unintended consequences. We are outlining what a consumer journey could look like but acknowledge much more work across sectors is needed to develop the final dispute resolution system.

CASE STUDY:

Simple scam still results in complex dispute resolution

Scam occurs: Amy receives an ad on Facebook saying that Telstra is offering compensation for affected customers in her area. She clicks on the ad, enters her phone number and then receives an SMS that has 'Telstra' as the sender ID. The SMS has a link for her to enter her bank account details so she can receive compensation. After entering her details, $7,500 is deducted from her account.

STAGE 1 Initiate Process

Consumer

Consumer contacts their bank.

Sending Bank

The bank issues a recall request from the receiving bank, but after 2 weeks, the receiving bank responds saying that money is already gone.

Sending Bank

Customer's bank then seeks to determine if this is a scam under the SPF definition and that the Consumer is a SPF consumer. This takes 2 weeks as the bank IDR team is busy with lots of applications on foot.

Sending Bank

Bank determines this is a scam and initiates an investigation. In our experience, this can take many weeks to conclude. Bank says the money has gone. Provides information on how customer can take better care next time.

STAGE 2

Internal Dispute Resolution

STAGE 2 Internal Dispute Resolution

Consumer

Consumer commences Internal Dispute Resolution.

Sending Bank

Telstra

- Bank contacts **Telstra**. Telstra says that it wasn't their service that allowed the SMS to impersonate them.

Facebook (Meta)

- Bank contacts **Facebook** who says they will only speak with their account holder.

Receiving Bank

- Bank negotiates with **receiving bank** which offers to pay 5% of the loss for not acting quickly enough.

Sending Bank

After a further e.g. 8 weeks we could see the, bank offer 10% goodwill payment to customer together with the 5% from receiving bank (15% total) on condition of customer signing a Non-Disclosure Agreement.

- EM 1.197 refers to IDR purpose to encourage early resolution but this process in the absence of the right incentives, can sometimes lead to low "goodwill" offers rather than genuine offers of settlement, potentially failing to achieve the intended goal.
- NB in our experience a consumer would have given up by now, often accepting very low goodwill offers because they are told by their bank that they are to blame for the scam.

STAGE 3

Seek Advice

STAGE 3 Seek Advice

Consumer

Consumer rejects offer and looks to make a complaint with AFCA which is, according to EM 1.203, "a pathway for redress... where a regulated entity has not complied with their obligations under the SPF". The Consumer must find evidence to prove that a/multiple entities have not complied with their obligations under the SPF. Consumer calls CALC for advice.

CALC Lawyer

Due to the complexity of the SPF, it takes the CALC lawyer 3 hours to review, research and explain to the Consumer their limited rights and how each party might be liable under each different SPF obligation. The lawyer explains that the business must have a scams policy in place and have taken steps to act on scams intel – this could be like Meta using software to identify scam ads. The Consumer can't tell if these obligations are met, although they know that any measures in place failed to prevent the scam.

CALC Lawyer

Lawyer tells Consumer they can lodge the complaint in AFCA and that they should also request evidence of:

- Actionable scam intelligence
- Reasonable steps taken to act on the scams intelligence
- The steps being taken in a timely manner
- Scams policies in place
- Relevant SPF Code requirements e.g. timeframes in place etc, i.e. elements not in a individual firm's scams policy

Consumer doesn't really understand the content of each of the SPF obligations but types the words referred to by the CALC lawyer into the AFCA complaint portal and requests this evidence from the banks and Meta.

Sending Bank **Receiving Bank** **Facebook (Meta)**

The banks and Meta, in our experience, are likely todecline to respond because there is now an AFCA complaint on foot.

STAGE 4

AFCA Complaints

Consumer Journey under **SPF**

Consumer Journey under a **Reimbursement Framework**

STAGE 4 AFCA Complaints

Consumer Journey under **SPF**

AFCA looks at the IDR outcome and sends the Sending Bank and Consumer back to IDR to attempt to resolve the dispute on better terms.

After another 4 weeks, sending bank maintains they have met all their SPF and Code obligations and the scam was caused by Facebook's error and declines to offer more money to customer.

Consumer calls CALC again. Consumer can't tell if the bank has met its obligations. CALC tells Consumer to inform AFCA that the dispute didn't settle. Consumer does so.

AFCA joins all the parties to the dispute:

Sending Bank | Receiving Bank | Facebook (Meta)

The correct Telco party is added, without having had a chance to resolve at IDR. For efficiency's sake, the Codes allow AFCA to proceed with EDR.

Telco

Consumer and AFCA asks each firm to identify when they received relevant 'actionable scam intelligence' and how they acted upon it. Possible responses on these facts could be as follows:

Sending Bank

- Sending bank says that they followed their obligations, and Facebook is to blame. Consumer has no evidence to prove otherwise.

Facebook (Meta)

- Facebook says that they provide a general warning that the ad wasn't verified. Consumer doesn't recall the ad warning and thinks they wouldn't have clicked if there was a warning, but doesn't have proof either way.

Telco

- The telco says the SMS ID registry is voluntary and it has no obligation to stop alpha tags being used. Consumer can't prove or disprove this but does have the text message.

In a worst-case scenario, AFCA may need neeeds to set up four separate conciliations:

- Consumer v Sending Bank
- Consumer v Receiving Bank
- Consumer v Facebook (Meta)
- Consumer v Telco

NB a consumer may again give up here as it's not worth the time off work and stress of 4 complaints.

The conciliations are arranged in close succession. The complainant has to take off work. Each party has to allocate resources to attend the conciliation.

At conciliation a possible result would be the businesses each offer to contribute 10% (40% total) leaving the Consumer paying 60% of losses, having lost much more in lost income and stress.

Matter then proceeds to determination – this could take some time if there are delays or backlogs at AFCA due to the likely high volume, multi-party and complex cases it must work though, particularly as the SPF is in its early years.

STAGE 5 AFCA Recommendation

STAGE 5 AFCA Recommendation

Sending Bank | Facebook (Meta) | Telco — The Sending bank, telco and Meta produce a certificate to AFCA that they met their obligations.

Receiving Bank — The receiving bank admits it didn't act in a timely way.

The businesses finally produce limited evidence to AFCA, or AFCA uses powers to request production of documents from the businesses or NASC. No evidence is provided to the Consumer.

It is possible that, based on the evidence, AFCA cannot confirm that the banks, Telco and Meta have met all of their obligations under the SPF and Codes. On this basis AFCA may determine the receiving bank should pay 10% of the money lost. AFCA has no other evidence to rely on, so on balance, it accepts the businesses' assertions.

After trying to push this case for a very long time, in this example, the Consumer is left with just 10% reimbursement, the two banks, telco and platform have each paid e.g. $8,000 ($32,000 total) for the case to go to full determination, in addition to staff costs of handling the dispute over the protracted period.

Consumer calls CALC again, distressed. They have lost all faith and confidence in the system and had to reduce hours at work due to the mental strain of this "relatively minor" scam. CALC lawyer advises the Consumer they could go to Court, but the Consumer gives up this time.

Consumer Outcome

All up the dispute could take over two years to resolve leaving the consumer recovering a fraction of money lost to scams

Consumer Journey under a **Reimbursement Framework**

Consumer

Consumer contacts their bank and provides all reasonable information they have about the scam.

Sending Bank

The Sending bank issues a recall request to the receiving bank account, but the Receiving bank says that money is already gone.

Sending Bank

The Sending Bank reviews information to ensure no fraud or gross negligence and refunds the Consumer within e.g. 10 business days as required under the Code.

Consumer Outcome

Consumer receives reimbursement in two weeks

Sending Bank

The Sending Bank then claims apportionment according to agreed industry default liability amounts: 25% Facebook for hosting the scam ad, 25% telco for sending scam text message, 30% receiving bank and 20% sending bank.

- 30% Receiving Bank
- 25% Facebook (Meta)
- 25% Telco
- 20% Sending Bank

Agreement is reached quickly because of the commercial nature of the settlement.

APPENDIX B – Scam survey results

Essential Research Polling Results – July 2024[57]

- A big majority of Australians (76%) believe if the law forced banks to reimburse, it would be a good incentive for banks to improve their technology to prevent scams.
- A big majority of Australians (75%) believe the law should require banks to refund scam victims if the bank hasn't kept their money safe.
- A majority of Australians (64%) believe it's the banks job to keep customers money safe, even if it is stolen as a result of customer being tricked by an online scam.
- A majority of Australians (60%) believe Australian law should require banks to refund all scam victims who have been manipulated into transferring their money online to a scammer.
- A huge majority of Australians (88%) believe online scams are getting more sophisticated and that anyone can be a victim, even if they are careful (over 55's 91%)
- A huge majority of Australians (87%) believe there is an increasing number of people in Australia falling victim to successful scams (over 55's 92%)
- Less than a third (32%) of Australians believe Australia is 'on track to have the best anti-scam regulations in the world'
- A majority of Australians (54%) think it is true that Australian banks reimburse only 2-5% of lost scam money.

[57] See: https://consumeraction.org.au/polling-big-majority-of-australians-say-banks-should-do-their-job-and-take-responsibility-for-keeping-our-money-safe/

APPENDIX C – Additional case studies from across Australia

Case Study – CCLSWA

Issues: vulnerability - English as a second language, elderly; bank warnings not effective to prevent scam loss but relied upon to refuse compensation

Jane*, an elderly client who speaks English as a second language, transferred approximately $500,000 over various transactions to scammers overseas. Jane was not transferring money for investment purposes, but rather due to her fears of the consequences in not doing so based on significant pressure she was put under. One of the banks involved is currently denying liability based on the warnings they provided to Jane.

Jane was coached by the scammers to say 'no' to various questions from the bank and Jane's first two transfers were processed.

In relation to the third large transaction to an overseas scammer, the bank advised that their staff member told Jane about scams and advised that the bank does not refund or reimburse scam transactions. The bank advised they recommended that Jane avoid interacting with unusual phone calls, text messages and emails and not to share SMS codes or any details pertaining to online banking.

The bank stated that Jane acknowledged that she understood this, and the transfer was then processed. As such, Jane is not entitled to be reimbursed.

CCLSWA submits that the bank did not take either appropriate preventative action nor more timely investigation and recovery action, especially due to:

- the number of "red flags" in this matter, in particular the volume and velocity of the transactions in question and the vulnerability of our client; and

- it being known that scammers will coach victims on what to say when speaking to their bank.

CCLSWA is seeking Jane's instructions to escalate the matter to AFCA as CCLSWA believes the bank should have been on notice of a real or serious possibility of a scam and should have made additional inquiries.

Jane's story is indicative of where a bank appears to have concerns a customer may be in the process of being scammed, that they can seek to avoid liability with a simple tick the box exercise of asking the customer whether they are being scammed.

*Not her real name

Case Study – CCLSWA

Issues: AFCA process unearthed substantially more information from the bank than was disclosed at IDR and whether it had a significant impact on the outcome or not; bank failing to have appropriate daily banking limits;

CCLSWA assisted Nelly, from a regional area, who had been the victim of a text message scam. Nelly was scammed out of her entire savings ($185,000) through multiple transactions.

Nelly received a text message saying that if she had not purchased a laptop on an account she had with a certain company, she should call a number provided. Nelly called the number and confirmed her name, date of birth, and the end of her credit card numbers with the scammer. The scammer then told Nelly that they were processing a refund and that she would receive a text message and that she should read out the code in the text message. The scammer then said they were having issues processing the refund and asked for further codes sent to Nelly's phone.

The bank denied liability, as Nelly had disclosed SMS pass codes to the scammer to facilitate the multiple transfers.

There were issues with how the bank dealt with Nelly's matter. This included misrepresentation to her in relation to her daily banking limit and unauthorised transactions.

CCLSWA assisted Nelly with an AFCA complaint and through the AFCA conciliation process. Amongst other things, claiming:

- the transfers where "unauthorised" transactions under the ePayments Code;

- the victim did not transfer all passcodes;

- the disclosures were not voluntary; and

- the multiple failed log in attempts and multiple large transactions should have been a red flag for the bank; and

- the bank had misled the client about the transaction limits on the account.

In its preliminary recommendation, AFCA found entirely in favour of the bank. It found that the due to the pass code breaches the client was liable. Further if found that the 'credit card limits were clearly outlined in the terms and conditions'.

The case progressed to determination. CCLSWA made further submissions and ultimately the Ombudsman agreed that:

- the terms and conditions on the transaction bank account were misleading as they did not make clear that for online purchases with a visa debit card the limit was the funds available in the account; and

- the transactions were unauthorised in accordance with the ePayments code, and while Nelly had disclosed the pass codes, taking into account 11.9 of the ePayments code (giving AFCA discretion to reduce liability) the bank should also have liability as no reasonable or other periodic transaction limit was applied.

The AFCA determination found substantially in Nelly's favour and Nelly received about $140,000 plus interest in compensation from the bank for the bank failing to have appropriate account limits on Nelly's bank account.

*Not her real name

Tessa's* story – Financial Rights Legal Centre (S311927)

Tessa started a relationship with someone who suggested she start investing in cryptocurrency. She subsequently began investing with a cryptocurrency platform and when she went to withdraw her money she was told she had to deposit an additional amount to withdraw her money, which she did. She attempted to withdraw money again but again she was told she had to deposit a further additional amount, which she did. Tess lost a total of over $30,000 AUD to the scam.

Tess had used her bank account with a big four bank to make the above transactions. At no point during this period did her bank flag these transactions as suspicious or try to contact her about these transactions

*Not her real name

Ursula's* story – Financial Rights Legal Centre (S310909)

Ursula is single and lives on the aged pension.

Ursula recently fell prey to an online investment scam and lost about $100,000. Ursula said she was caught up on the promise of returns to the value of $300,000 which she never received

Ursula's (big four) bank allowed the payments through despite at one point having had a conversation with Ursula to the effect that this account may be a scam. Ursula did not take any notice of the warning.

*Not her real name

Amy's* story – Financial Rights Legal Centre (S305628/S308740)

Amy received a spoofed text message on the same chain as her legitimate bank messages, asking her to contact a number if she had not requested a verification code (which she had not).

Once Amy called the number, and someone explained that multiple devices attempting to access her account and it needed to be blocked. Amy gave her username and some verification codes to the scammer and proceeded to get locked out of her account and have a new device, not belonging to her, granted access to her account. The scammer changed Amy's daily payment limit and over $45,000 was debited out of Amy's account into another account with the same bank, without Amy's knowledge or consent. As the funds were quickly moved again and then withdrawn, they could not be recovered.

Amy's bank was unable to detect and block the transaction, even though there was a login from a completely new device, with an instant change in daily payment limit and instant transfer of a large lump sum to a new account. The bank also continues to use SMS for communication, knowing that this has been compromised due to various fraud victims' cases in the past. There were no safeguards available to suspend suspicious transactions.

The bank withheld compensation in part in reliance on ineffective warnings, including:

(a) a broadcast "scam warning" SMS sent to customers before Amy became a customer, and

(b) SMS warnings that provided an OTP code and requested the customer to call the bank if not requested, but did not explicitly tell customers not to disclose the OTP code to the bank.

*Not her real name

Weir's* story – Financial Rights Legal Centre (S310952/S306350)

Within the last 2 years, Weir, an Aboriginal pensioner living rurally, made an $8,000 payment to an account with another bank believing he was paying a genuine invoice. At the time he made the transfer, Weir was not aware he had fallen victim to an invoice hacking scam. Soon after, Weir discovered he had been scammed and reported the disputed transaction to his (big 4) bank. The bank was unable to recall the funds.

Weir says if the bank had taken appropriate and timely action when he reported the scam, his funds would have been recovered and wanted the bank to compensate him. The bank offered Weir half the amount as a goodwill payment to resolve the complaint. Weir rejected the bank's goodwill offer.

AFCA found that the bank did not make any errors or breach its obligations to the Weir when it processed the disputed transaction. The bank processed the disputed transaction according to Weir's instructions, as there was nothing known to the bank about the disputed transaction that put it on notice of the scam.

Weir's bank was however found to have made an error in recalling the disputed transaction. Weir had reported the disputed transaction as "fraud related" and therefore his bank should have pursued the recall as fraud related and not as "goods not received". However, there was insufficient information to indicate it is likely that had the bank recalled the disputed transaction as fraud related it would have been successful in recovering the disputed transaction, so it was not liable for financial loss. This despite the substantial amount of time the receiving bank took to respond to the sending bank's notification.

AFCA decided that the sending bank's error caused significant emotional damage to Weir for which the bank should pay non-financial loss. The bank had offered 50% of the financial loss and AFCA endorsed this as part of the determination.

*Not his real name