

06 February 2023

By email: [paymentsconsultation@treasury.gov.au](mailto:paymentsconsultation@treasury.gov.au)

Director – Payments Strategy and Policy Unit  
Financial System Division  
The Treasury  
Langton Crescent  
Parkes ACT 2600

Dear Treasury

## Joint submission: A Strategic Plan for the Payments System

Thank you for the opportunity to provide input on the development of the Government’s strategic plan (**Strategic Plan**) for the payments system. This is a joint submission by Consumer Action Law Centre (**Consumer Action**) and Financial Rights Legal Centre (**Financial Rights**).

We consider the safety and resilience of the payments system to require urgent attention and intervention and outline the reasons for this below. The increasing prevalence of fraud and scams operating within our payments system in particular is a major concern for the clients we represent. Our casework experience indicates that there are a number of areas where the digitisation of banking and finance has created gaps in the security of the payment system that scammers can exploit.

We have been calling the banking industry and payments system to take more responsibility to ensure that scam victims are reimbursed by their banks when they lose money as a result of being tricked into transferring money using banking and payments platforms. We note that the ACCC has recently called on the banking sector to take more responsibility for preventing and detecting scam transactions and to reimburse customers for their scam losses—a call we strongly support.<sup>1</sup>

Furthermore, the Organisation of Economic Development (**OECD**) and the G20 recently updated its High-Level Principles on Financial Consumer Protection.<sup>2</sup> These updated principles include a new principle of “protection of consumer assets against frauds, scams and misuse”, noting that “protection mechanisms should include clear and transparent liability arrangements between financial service providers and consumers in the event of financial loss”. This should be taken into account in finalising the proposed strategic plan.

While we support the development of a strategic plan for the payments system as set out in the consultation paper (**Paper**) and the roadmap proposed, there are more initiatives that could be included that are absent from the Paper. Primarily, we urge the Government to use the Strategic Plan to help identify where intervention is necessary to improve consumer outcomes, namely where market forces in the payments system are not delivering this alone. At present, this is particularly needed in regard to the safety and security of the payments system, most obviously evidenced by the recent major increases in losses and consumer harm caused by scams and fraud.

A summary of recommendations is available at **Appendix A**.

<sup>1</sup> <https://www.theguardian.com/money/2023/feb/01/australian-banks-should-reimburse-scam-victims-acc-and-consumer-advocates-say>

<sup>2</sup> See: <https://www.oecd.org/finance/high-level-principles-on-financial-consumer-protection.htm>

## Question 1: key principles for the payments system

We generally support the four key principles set out in the Paper, and recognise each needs to be fostered to deliver an effective payments system that delivers good outcomes for everyone. However, we also recommend that 'fairness' be added as a fifth principle. There is also a particular pressing need for government action and intervention in relation to the trustworthiness of the payments system.

### Trustworthiness

We strongly support the inclusion of 'trustworthiness' as a key principle of the Strategic Plan. Of the principles listed in the Paper, it is the one where there is the most obvious need for targeted improvements at present, particularly in terms of safety and security. We accordingly address the current need for this further in response to question 2.

Trustworthiness must be a key principle in the Strategic Plan in recognition that it can not always be delivered by market forces alone. A number of the initiatives listed in Attachment B of the Paper will help improve the trustworthiness of the payments system. However, there are additional areas for improvement the Government should be considering that are not listed, including those we have proposed below in response to question 4.

### A fifth principle: fairness

We urge the Government to recognise and include fairness as a separate and equal key principle to underpin the future direction of the payments system. We consider a fair payments system to be one:

- That ensures payment functions and services are designed and implemented clearly and honestly and cater to the diverse literacy, cultural and educational standards of all consumers;
- That does not distort or unduly influence consumer choices about payment mechanisms that suits their needs and preferences;
- In which the for-profit businesses that operate in it do so honestly and on reasonable terms (and in which there are laws to require this); and
- That ensures advancements do not restrict accessibility for portions of the population, particularly those experiencing a form of vulnerability.

While fairness would sometimes be captured by the four principles proposed in the Paper, the other priorities can also conflict with it in some circumstances. For example, ensuring accessibility to the payments system for all users is a goal consistent with ensuring the system operates fairly for everyone. However, applying this principle to ensure simpler business access (such as where the Paper refers to removing barriers to entry) needs to be balanced against the need for consumer safeguards. Consumer safeguards work to ensure that services are rolled out in ways that make them available to all segments of the population, or when services are withdrawn this is done so in ways that do not negatively impact upon vulnerable cohorts, for example for those who continue to rely on cheques. We hold similar concerns that the principles of efficiency or innovation can be pursued without specific regard for fairness.

Fairness needs to be included as an additional principle to ensure that fair outcomes for all Australians are not displaced or forgotten when other principles suggest an alternative direction. Fairness will be particularly important as consumers are forced to move towards a predominantly digital economy. In the transition to a digital economy, certain segments of the population are at greater risk of being left behind by this change, such as older people, people with disabilities or culturally and linguistically diverse communities. As stated in the Paper, the payments system has become significantly more complex in recent years, but reasonable use remains fundamental to everyone in society.

**RECOMMENDATION 1.** Add 'fairness' as an additional key principle to guide the future of the payments system.

## Question 2: key priorities for the payments system

The key priorities proposed in the Paper are sound and logical. We make specific comments about some of the priorities below.

### Safety and resilience

Consistent with our comments above regarding the trustworthiness principle, we consider the safety and resilience of the payments system to require urgent attention and intervention. We hope that its inclusion as the first priority listed in the Paper indicates an intention that the government and the Strategic Plan will treat it as the leading priority for the near future.

Recent developments in the payments system have no doubt seen major advancements to its efficiency and convenience. Today, there are generally numerous options available to people and businesses that allow for near instantaneous electronic payments. Contactless payment and electronic wallets have become commonplace, and Australian companies have developed recent alternate payment methods that are now popular across the world, such as buy now pay later (although this should primarily be considered as a credit product, rather than a payment method).<sup>3</sup>

We don't seem to be lacking for innovation in terms of making things faster and more convenient. By comparison, the reliability and safety of these systems has not always improved with these enhancements and in some cases has suffered indirectly as a result of specific advancements targeted at these other principles.

The increasing prevalence of fraud and scams operating within our payments system in particular is a major concern. In late 2022, the ACCC estimated that \$4 billion in Australia would be lost to scams that year<sup>4</sup>—an amount which doubled the amount lost in 2021,<sup>5</sup> which had also more than doubled the previous year.<sup>6</sup> These kinds of scams must involve the payment system—while the scammer-victim relationship may originate elsewhere, the scammer must know they can access the victim's funds held in the payment system.

Our casework experience indicates that there are a number of areas where the digitisation of banking and finance has created gaps in the security of the payment system that scammers can exploit. For example, while the speed that transactions are processed at now is certainly convenient, it also means that a scammer can receive money in Australian account then transfer it out of the country so fast that even if a victim recognises they have been scammed almost immediately, the money is often already gone. Other gaps may have always existed but have recently become known by scammers, or easier to take advantage of. Further examples of these are provided below in our feedback regarding the initiatives that could help address them, at question 4.

The Strategic Plan should be a tool to help address these issues as it is not clear market forces are delivering a sufficiently safe and secure payment system alone.

**RECOMMENDATION 2.** The Strategic Plan should recognise recent trends that indicate the payments system is most in need of interventions targeting improvements to its safety and security in the medium term.

---

<sup>3</sup> See our submission to Treasury's consultation on Regulating Buy now, pay later in Australia here: [https://financialrights.org.au/wp-content/uploads/2023/01/221223\\_BNPLOptionsPaper\\_JointConsumerSub\\_FINAL.pdf](https://financialrights.org.au/wp-content/uploads/2023/01/221223_BNPLOptionsPaper_JointConsumerSub_FINAL.pdf)

<sup>4</sup> <https://www.accc.gov.au/media-release/scams-awareness-week-2022-empowers-australians-to-spot-a-scam-o>

<sup>5</sup> ACCC, *Targeting Scams: Report of the ACCC on scams activity 2021*, July 2022, available at:

<https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf>

<sup>6</sup> <https://www.accc.gov.au/media-release/scammers-capitalise-on-pandemic-as-australians-lose-record-851-million-to-scams>

### Question 3: Key initiatives proposed as part of the Strategic Plan

We generally support the broader initiatives listed, though we provide recommendations about elements of the detail (and raise some concerns) in response to question 4.

### Question 4: Feedback on approaches to the initiatives

We provide comments on relevant initiatives listed in Attachment B below.

#### Reduce the prevalence of scams and fraud

We strongly support the inclusion of this initiative and consider it to be a vital areas of focus. However the level of detail and substance proposed by some of the actual actions contemplated in Attachment B of the Paper needs to be significantly improved.

#### ePayments Code

We strongly support the proposal to mandate the ePayments Code and for the Strategic Plan to set out a roadmap for this process. For this to deliver effective results however, the flagged consultation process must be sufficiently scoped to consider the appropriate application of the ePayments Code in relation to scam prevention. Recent changes to the definition of 'mistaken internet payment' in the ePayments Code expressly clarified that many key protections in the ePayments Code do not apply to transactions a consumer initiates due to a scam. This, along with the prevailing interpretation to other existing finance laws, means there is a glaring absence of meaningful obligations upon financial firms to protect their customers from scams, and no consequences if they fail to do so. The next section addresses the need for this to be rectified more generally—amending the ePayments Code is one place where meaningful consumer protections could be introduced that would impact many scams.

#### Develop overarching obligations on payment platforms to protect their customers from scams

There are currently no clear standards that oblige banks to detect or prevent scam activity. Whether they sit in the ePayments Code or elsewhere, there is a desperate need for clear and meaningful obligations to be imposed upon banks and other financial firms to protect consumers from scams.

The current prevailing interpretation of existing laws that arguably could impose a standard of care in this regard have been read down by the banks and the Australian Financial Complaints Authority (AFCA), such that at present, losses from scams are generally solely borne by the victim.<sup>7</sup> The absence of any liability on the financial firm in this regard is different to other kinds of financial crime like unauthorised transactions (such as credit card fraud), and has led to inconsistency in how banks approach this issue—both in terms of prevention, and in handling the losses suffered by customers. So, while use of the payments system in some way is essential for scammers, laws need to be strengthened so that the banking industry takes on more responsibility for preventing scams and reimbursing victims who incur losses using payment systems.

The Paper correctly recognises that the private sector is “the first line of defence against scams”. Payments systems companies (especially banks) have a wealth of transaction data available to them to help monitor and identify scams. While it may not be possible to prevent all scams, in our view a clear problem exists when there are no clear standards on what the “first line of defence” should do, or any penalties for failing to meet the standards.

---

<sup>7</sup> See for example recent AFCA determinations 868100 and 897711, available at <https://serviceo2.afca.org.au/CaseFiles/FOSSIC/868100.pdf> and <https://serviceo2.afca.org.au/CaseFiles/FOSSIC/897711.pdf>. AFCA determinations commonly contain statements similar to this (taken from determination 897911): “There is no law or banking industry practice which requires the bank to monitor or scrutinize its customers transactions to ensure they are free from scams or fraudulent conduct.”

## Case Study – Ryan’s story

Ryan (name changed) called us after falling victim to a threat-based scam . He told us he received a call that appeared to be from a number he had received legitimate text messages from his (big 4) bank on before, and was told that his account had been compromised and he needed to transfer his money to a new account.

Ryan said in line with instructions over the phone, he made 9 transactions to a new account, totalling nearly \$40,000 – instructions he now knows were from a scammer . He said that the same day this happened he realised he may have been scammed, and called his bank but waited on hold for over 2 hours before getting onto their fraud team, by which time the money was gone. The bank attempted to recall the funds that same day, but was unsuccessful. The bank assessed his case and said that, despite his entire bank account being quickly drained over a short period of time and making no direct contact with him to confirm these transactions, it didn’t trigger their scam detection system, and that they acted reasonably in their response. As such, they had no liability to the client. The bank did however make him a ‘goodwill’ offer of a few thousand dollars to settle his complaint , but this did not meet his significant losses.

We recommend that financial firms be required to reimburse their customers where they fail to prevent scammers from obtaining their money via their payment platforms. Such an approach would:

- Create a financial incentive for banks and financial firms to invest in more resources to develop systems to better manage the risks that exist in the modern payments system, and
- Be more consistent with reasonable societal expectations that diligent and skilled bankers or financial service providers would be obliged to keep their systems safe and their customers protected.

This approach has been taken by a number of banks in the UK—with many of the major banks signed up to the Contingent Reimbursement Model Code (**CRM Code**)—in which they commit to reimburse victims of authorised push payment scams in the majority of situations.<sup>8</sup> This has incentivised the banks to do more to prevent scams, and indeed some steps taken (such as checking if the recipient account name matches the sender’s intended recipient) have resulted in losses to some types of scams reducing there.<sup>9</sup> Recent data indicates a majority of customers of signatory banks that fall victim to scams are being reimbursed,<sup>10</sup> and this has certainly not led to financial disaster for the banks.

The Payment Systems Regulator (**PSR**) in the UK is currently consulting on a proposal to make a commitment to reimbursement mandatory,<sup>11</sup> with related (Government-led) legislation currently before UK Parliament to enable this approach.<sup>12</sup> Part of this proposal would see liability sit 50-50 with sending and recipient banks as a starting point—which reflects the ability of both to take steps to prevent scammers using their platforms or targeting their customers. UK consumer group *Which?* made a submission to this consultation that emphasises how important it is for banks to be incentivised to stop their accounts being used for fraud, particularly on the receiving end—as this is the scammer’s access into the payment system.<sup>13</sup> Currently there are few if any incentives placed on Australian banks to take proactive steps to stop their accounts from being used for fraud. This is because they bear little risk or liability for the results of scams that occur over flawed payments systems that they require customers to use.

<sup>8</sup> <https://www.lendingstandardsboard.org.uk/crm-code/>

<sup>9</sup> UK Finance, *Annual Fraud Report: The definitive overview of payment industry fraud in 2021*, see for example Invoice and Mandate Scams statistics (p 60), available at [https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022\\_FINAL\\_.pdf](https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf)

<sup>10</sup> Ibid, page 49.

<sup>11</sup> <https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/>

<sup>12</sup> <https://bills.parliament.uk/bills/3326>

<sup>13</sup> Which? response to PSR consultation on APP scams: Requiring reimbursement, available at: <https://www.which.co.uk/policy/money/3552/consultation-responses-payments>

The PSR's proposed model would contain far fewer exemptions to the presumption that a scam victim will be reimbursed than exist in the CRM Code – with the only exemption being 'gross negligence'. The precise meaning of this term is not clear, but it appears likely that a customer's decision to ignore a specific and tailored warning from a bank about the identified risks of a transfer would be one such example – a limitation that would reduce the risk of banks being unable to act to mitigate their losses.<sup>14</sup>

Separate to this, mid-size UK bank TSB has of its own initiative established a 'fraud refund guarantee', whereby it commits to refund all their customers who fall victim to scams.<sup>15</sup> They rely on even fewer exceptions than exist in the CRM Code, and report an even higher rate of refunds.<sup>16</sup> TSB publicly endorse this approach as a beneficial option for their business to help them improve client safety—including in a webinar hosted by Consumer Action on 1 February.<sup>17</sup> As noted above, while the industry has moved toward faster and faster payments and an altogether frictionless system, TSB recommend consideration of the benefits of introducing more friction into the system to give banks and customers more time to identify and respond to fraud or scams.<sup>18</sup> This could involve a move away from instant transfers and more proactive quarantining of funds by banks when transactions are unusual or suspicious.

There have been concerns raised about the risk that if banks were on the hook for the financial losses of scams, that this might risk making Australia a 'honey pot' or easy target for scammers. TSB's experience suggests that if anything, the opposite is the case. TSB has repeatedly publicly dispelled the 'moral hazard' claim, finding no evidence that their customers are any less careless with their money. In fact, TSB report lower fraud loss rates than the broader UK banking industry. It also creates the financial incentive for the bank to do more to prevent losses – something that is obviously lacking from our current model.<sup>19</sup> Scammers don't care who foots the final bill for scams – they only care about how difficult it is to get the money, and incentivising the banks to make this harder is the best way to make Australia less attractive to scammers. Consumers will always do everything they can not to be scammed, even if they thought the financial risk was removed. Our clients who have fallen victim to scams express significant embarrassment, shame and frustration about the experience. Nobody wants to be duped, deceived or misled.

#### Concerns about 'fairness' of reimbursement

Another common concern raised about a bank reimbursement model relates to fairness – and whether it is reasonable for banks to be liable for losses in most situations.

Someone has to pay for scam losses and unless it is the scammers it is inevitably going to be "unfair". However, we consider a model where banks reimburse to be a significant step towards fairer than the current situation, where individual victims of scams cop the losses themselves.

As we say throughout this submission, the prevalence of scams is an indirect outcome of a faster, more digitised payments system. Many steps in establishing bank accounts and making transfers have been fasttracked in the last 30 years, often involving doing away with steps that were for security or fraud prevention. While society has called for it, we have been led to understand that industry considered these changes to be safe.

The prevalence of scams obviously demonstrates that there were compromises as a result of these changes, to the point that now that the safety of online banking has limits, and scammers have significant access to Australian banking platforms. These are things that consumers cannot change, and with the increasing complexity seen with scams, it is becoming very difficult (sometimes virtually impossible) for consumers to identify and avoid scams.

---

<sup>14</sup> <https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/,page7>

<sup>15</sup> <https://www.tsb.co.uk/fraud-prevention-centre/fraud-refund-guarantee>

<sup>16</sup> Ibid.

<sup>17</sup> A recording of this webinar can be provided upon request

<sup>18</sup> TSB Bank, *Tackling fraud together report*, April 2022, available for download at: <https://www.tsb.co.uk/news-releases/tsb-marks-three-years-of-fraud-refund-guarantee/>

<sup>19</sup> Ibid, pages 4 and 8.

Worse still, people experiencing vulnerability are more susceptible to scams. This applies both to people who are structurally vulnerable – such as the elderly, cognitively impaired, poorly educated, as well as to people who are situationally vulnerable, which is why scams are designed to catch us at a particular moment when we are likely to be more susceptible to (for example) a threat, or an emotional, quick reaction. Accordingly, scams currently contribute to broader inequality in society.

A model where banks reimbursed blameless customers would be fairer in this regard and provides motivation to all involved to stop it from happening. Further, if the financial services industry was made to bear the cost, this will still be passed onto consumers eventually – as the costs will be worked into the industry business models. However, this would permit the costs to be borne evenly by society more broadly, rather than just the vulnerable and the unlucky. It would also ensure that the industry is doing all it can to stop these losses.

Certainly, banks are not alone as the only entity involved in this issue. The UK is also currently exploring the role of other major institutions whose platforms scams often originate on, such as telcos, social media giants and messaging platforms, and requiring them to do more as well. While this may lead to a more broadly shared approach to liability (which would likely get us closer to a status resembling “fair”),<sup>20</sup> there has been recognition in that jurisdiction that this should not delay the introduction of material standards on banks in this space.

#### Broad consultation when mandating of ePayments code

We recognise that the Strategic Plan may not be the vehicle to deliver drastic changes in policy. However, for all the talk in this Paper (and more broadly by the Government) about trustworthiness, safety, resilience and scam prevention to have any real impact, it should at least set out a timeline for examining this issue.

Consultation as part of the process of mandating the ePayments Code could be one way such obligations could be introduced (provided the consultation was sufficiently broad to consider the substance of the Code, not just changes technically necessary to mandate it). However, this would still leave scams not involving ePayments (such as where a victim is persuaded to transfer money in branch) untouched, and may require addressing elsewhere.

#### **Case Study – May’s story**

May (name changed) engaged a conveyancer to help with settlement for a home she bought. She told us that she transferred the conveyancer her deposit (of over \$100,000) per emailed instructions. To do this she said she had to go to her local bank branch. She told us that she later found out that the conveyancer’s email had been intercepted or hacked and she had transferred the money to a scammer’s account.

May says she had been told by her bank that the money is frozen in the recipient (Australian) bank account, with both fraud squads working on it, but despite being ‘frozen’ it was not clear whether the money was recoverable and that it could take 4-6 weeks to work this out, leaving the property settlement in limbo.

It would also be essential that effective prevention of scams would also likely require ensuring equivalent obligations are imposed upon cryptocurrency operators, such as crypto asset secondary service providers (CASSPrs)—this is discussed further in response to question 7. Similar protections should also be considered for superannuation firms, where some AFCA determinations suggest a similar absence of current obligations exist.<sup>21</sup>

<sup>20</sup> <https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet>

<sup>21</sup> See for example recent AFCA determinations 77888 and 826592 for examples of cases where customers lost significant sums to scams and basic checks could have prevented their loss available at <https://service02.afca.org.au/CaseFiles/FOSSIC/778888.pdf> and <https://service02.afca.org.au/CaseFiles/FOSSIC/826592.pdf>

### Identify specific steps to help stop scams

From an economic perspective, introducing broad financial responsibility for scam losses on payment systems providers would likely be the most efficient way to ensure that the private payments sector is doing all it can to make their systems safe from scams. However, another way the Strategic Plan could meaningfully reduce the prevalence of scams is to require that industry deliver upon specific protections aimed at disrupting scam activity.

There is a brief discussion in Attachment B about the introduction of new technologies that can help improve security and make it harder for scammers to operate. However, the actions section appears to indicate that the Strategic Plan will do little more than provide for supporting and monitoring this process, and seemingly will leave meaningful steps to the will of the private sector.

The rate that scams losses are increasing make it abundantly clear that the financial/payment private sector's response to the drastic increase in scams to date has been insufficient. This is precisely the area where Government intervention is required.

### Set a hard timeframe for retiring BECS and mandating confirmation of payee or PayID

While the Paper refers to the rollout and uptake of the New Payments Platform (**NPP**), it appears to only contemplate a very minor monitoring role in relation to this for the Government and the Strategic Plan.

The technology for the NPP has been available for years, but rollout has been unreasonably slow. As a result, the predominant platform for bank transfers remains the decades old BECS system—the limitations of which are recognised in the 'Support the transition to more modern payments infrastructure' section of Attachment B. The 'Actions' side of that section of Attachment B also seems to envisage a role supporting private sector led transition.

While it is standard practice to require customers provide a recipient name for bank transfers made using the BECS platform, banks do not check the name matches the recipient—often even if the recipient account is with the same bank. This creates a false sense that this is a safety measure for customers, and means scammers can trick people into transferring to accounts where the names do not match at all.

Sector-wide adoption of PayID would create an additional barrier for scammers as the platform provides the transferor with a prompt indicating the name registered to the recipient account, addressing this gap in security with the BECS transfer system. It is one way a 'confirmation of payee' safeguard could be delivered by industry.

Industry recalcitrance, obstruction and delay in pushing for a quick transition from BECS means that government needs to play a stronger role in the transition. The Reserve Bank of Australia and ACCC<sup>22</sup> has encouraged the uptake of this technology for years, but industry has dragged its feet. Unfortunately, the availability of NPP as an option won't help prevent scams until uptake is sufficiently high that BECS transfer requests become rare. Consumer Action has discussed confirmation of payee with the big 4 banks. While supportive of PayID, their experts are sceptical about the impact universal confirmation of payee would have on scammers as they believe it could be bypassed by the elaborate schemes and lies told to victims.

This may be true for some scams, but it should not mean that industry can avoid introducing a commonsense solution that will make it harder for scammers and address a significant proportion of current scams. Name-matching this would introduce a significant barrier for fraudulent invoice scams. In the UK the 10 biggest banks have largely adopted confirmation of payee technology, and in 2022 reported losses to invoice and mandate scams decreased by 17%.<sup>23</sup> While scams losses in the UK more broadly continue to increase, their reported losses are not doubling every year, and an economy much larger than ours reports lower scam losses overall.<sup>24</sup>

---

<sup>22</sup> <https://www.accc.gov.au/speech/making-australia-a-harder-target-for-scammers-keynote-address>

<sup>23</sup> [https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022\\_FINAL\\_.pdf](https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf), page 60

<sup>24</sup> Ibid, page 47. The UK reported approximately £583.2 million was lost to APP scams in 2021 (approx. \$1 billion AUD) – around half our estimated losses

In recent days, the Commonwealth Bank has indicated that it is taking steps to address this problem and will name-check customer accounts. This is a welcome move but safety should not be a matter of competitive advantage and choice of which bank you use. It should be a basic requirement of all banks and payment systems.<sup>25</sup>

### Case Study – Godfrey’s story

Godfrey (name changed) is a self-funded retiree who lives in the outer suburbs of Melbourne. In mid-2022, Godfrey contacted us seeking advice after he lost money to a fake invoice scam.

Godfrey told us that he was getting work done on his home and received an email invoice from the builder for over \$25,000, which he paid online. Godfrey said he later found out that a scammer had hacked his or the builder’s email, and had changed the BSB and account number details to another Australian account at another bank that was unrelated to the builder.

Godfrey was told that there was nothing that his bank or the recipient bank could do about the thousands of dollars lost.

**RECOMMENDATION 3.** As part of its initiatives addressing scams and fraud, the Strategic Plan should provide a framework for consulting on and introducing obligations for firms (including banks, super funds and CASSPrs) to detect and prevent scams on their payment systems. These obligations should impose financial responsibility for scam losses on system providers where relevant standards are not met.

**RECOMMENDATION 4.** The Government should use the Strategic Plan to set a timeline for mandating that banks introduce confirmation of payee technology, or otherwise provide customers with the ability to check the account name of a transfer recipient matches their intended recipient.

#### Set a timeframe for mandating all ADIs to share (and use) specific data to help scam prevention

Related to the development of the national anti-scam centre, another area where the Strategic Plan could provide meaningful direction for industry is in relation to the provision and use of data sharing for scam and fraud prevention. We understand that the big 4 banks plus some other banks currently have an arrangement with the Australian Financial Crimes Exchange (AFCX) and Scamwatch that allows for realtime sharing of data related to scams. Where possible, banks send and receive information that comes in regular updates.

This is a great initiative, however based on our understanding of it there are a few rather obvious shortcomings to this arrangement at present:

- Only some banks are involved
- There are no real obligations on what kind of information must be provided by banks
- There are no specific obligations on how the information received must be used (so there are no guarantees the process delivers meaningful outcomes).

There are no doubt a number of complexities to these arrangements in terms of how data is collected, privacy concerns and collection standards. However, sharing data from the payments system on scams directly is surely one of the most meaningful ways that scam can be identified and stopped across multiple platforms, quickly.

The value of industry sharing information on fraud and scam risks has been clearly identified in the UK and is another step that is being called for by consumer advocates such as *Which?* in that jurisdiction.<sup>26</sup> A platform

<sup>25</sup> <https://consumeraction.org.au/australias-banks-should-follow-cbas-lead-and-introduce-stronger-measures-to-stop-scams/>

<sup>26</sup> *Which?*, above n 11, p 30.

permitting this would also be useful to more accurately help assess appropriate distribution of liability between the banks involved in scam transactions where the money was lost.

We strongly encourage Treasury to engage with the ACCC and AFCX about the ways in which the Strategic Plan could assist in driving improvements to this process. Seeing a meaningful timeline for the expansion of this arrangement could lead to significant improvements in scam detection.

**RECOMMENDATION 5.** Treasury and the Government, in conjunction with the ACCC and AFCX, should explore ways in which the sharing (and use) of real-time transaction data on scams between banks can be mandated and fasttracked. This should be an initiative in the Strategic Plan.

## **Support the transition to more modern payments infrastructure**

### Retiring BECS

As mentioned above, we urge the Government to consider more proactive and forceful involvement in the adoption of more secure payment platforms, such as the NPP, to allow for the retirement of BECS, which remains a liability in terms of security.

### Intervention is required to provide consumer control over recurring payments

Recommendation 60 of the 2017 banking code review was that banks should work with card scheme companies to help make it easier for customers to cancel recurring payment arrangements that occur via cards.<sup>27</sup> This recommendation was supported in principle by the Australian Banking Association (**ABA**). Recommendation 80 in the 2021 Banking Code review made a similar recommendation.<sup>28</sup>

The difference in rights between cancelling a direct debit which is set up using a BSB and account number, compares to a direct debit using scheme card numbers (known as recurring payments) is, understandably, very confusing to consumers. More and more people are being encouraged to establish recurring payment arrangements using Mastercard or Visa facilities. The rollout of new security measure such as 'Tokenization' and Authentication also prevent new difficulties when trying to cancel recurring payment arrangements. We understand that even in circumstance where an individual is issued a new card, this may not result in payments being stopped.

A particular concern with the challenges in cancelling direct debits is that has a huge impact upon the financially vulnerable. This is exacerbated by some businesses which establish multiple direct debits. Some businesses authorise multiple direct debit authorities so when a consumer cancels one direct debit, the business moves on to use another authorisation in an effort to stymie the cancellation of direct debits by consumers. We are aware of some companies using up to eight authorisations.<sup>29</sup> The practice is particularly prevalent in the payday lending sector.

Five years after the 2017 Banking Code recommendation, the cancellation of recurring payments remains a difficult issue. Since then, the ABA has said that there are difficult and expensive barriers to this—some of which are beyond their control, and relate to the card providers (Visa, Mastercard). Outside of those who have found out the hard way, most consumers are not aware that arranging payments through a card as opposed to via direct debit can make cancellation far more difficult.

This is an issue that relates to providing consumers with fundamental control of their own money. For the majority of the population, the entities that have the power to change this are Mastercard, Visa and the big 4 banks. It cannot seriously be that complex an issue that these entities cannot solve. Clearly this is not being treated as a

---

<sup>27</sup> <http://cobpreview.crkhoury.com.au/wp-content/uploads/sites/2/2017/02/Executive-Summary-Independent-Review-of-the-Code-of-Banking-Practice-2017.pdf>

<sup>28</sup> <https://bankingcodereview.com.au/wp-content/uploads/2021/12/Final-Report-Banking-Code-of-Practice-Review-2021.pdf>

<sup>29</sup> We note for example, that Cigno's Third Party Direct Debit Authority Request includes eight direct debit user ID's of Ezidebit Pty Ltd: <https://cignoloans.com.au/third-party-direct-debit-agreement/>

priority by these companies. There is a desperate need for forceful intervention to put a stop to this issue that disproportionately impacts people in financial hardship.

**RECOMMENDATION 6.** The Strategic Plan should include pathways to resolving the issues that prevent people from cancelling recurring payments set up via cards, as a priority.

### **Support international efforts to enhance cross-border payments**

We support the general goal of making it easier for people to make international payments. This is an area that can be quite complex and a number of payment system market players charge significant fees that do not appear to have any real relationship with their costs, or offer uncompetitive exchange rates without any real justification.

That said, it is vital that enhancements toward this goal do not result in it becoming even easier or faster for scammers to get stolen funds offshore. Removing all friction should not be a key aim of the plan. Acknowledgement needs to be made that some friction in the payments system is important and a critical safety tool.

An all too common outcome when someone reports that they believe they have been the victim of a scam to their bank is that the money is already lost, even when identifying it almost immediately after a transfer is made. The majority of scams involving bank transfers we see involve transfers to another Australian bank account. Presumably, if the money was still in another Australian bank account, it could be traced and returned. Accordingly, we assume that most of the time, scams eventually involve transferring money out of Australia to where it cannot be easily tracked.

Scammers are criminals, yet they are rarely apprehended. Instead, we leave the financial responsibility with the victim, and the discourse too often appears focused only on asking what the victim could have done to protect themselves. Assuming all these scammers are working overseas, it would be disastrous if intentional advancements in cross-border payment systems made it easier for international criminal scammers to get money out of Australia. This may be an area where efficiency needs to be tempered to ensure it does not come at a cost to the safety and security of the payments system.

#### **Case Study – Perry’s story**

Perry (name changed) is in his 70s and lives in regional Victoria.

Last year he contacted us and reported that he fell victim to a remote access scam, where a scammer fraudulently convinced him to provide access to his computer and managed to access his bank account. While this was happening, he told us that Bendigo Bank contacted him and asked him if he had just transferred \$5000 from his account—which he said he did not. Perry recounted that the Bendigo Bank staffer told him he was being scammed and that a further amount of almost \$15,000 had been taken from a linked account while they were on the phone.

Perry said that he could see the first \$5000 transaction went to another Australian account, while the second went overseas. Yet, both were not able to be retrieved even though Bendigo Bank identified the scam in near real time. Perry ended up accepting an offer from Bendigo Bank to reimburse half his losses. When deciding whether to accept this, Perry said the police told him that they had tracked one transaction that went rapidly across two Australian accounts, before being transmitted to Turkey and it was unlikely to be recovered.

Perry said the loss definitely made things harder financially, but since settling the matter he was trying to forget about it, because it just left him feeling frustration, helplessness and anger.

## Question 5: Key milestones

We would like to see timelines for the following included in the Strategic Plan (to the extent that they are not progressed before the plan is published):

- A roadmap for consulting on the content of, and mandating, the ePayments Code;
- A process to consult on and review of the legal obligations that apply to payments platform providers such as banks to detect and prevent scams and fraud from occurring on their platform;
- The retiring of BECS and adoption of the NPP or similar technology including confirmation of payee;
- A mandatory timeline for industry (Visa, Mastercard and banks) to remove the barriers that make it difficult (or impossible) for people to cancel recurring payments made from their cards.

## Question 6: Proposed review process

The proposed review process appears sound, however the annual review cycle does seem ambitious for the whole plan, depending on the level of detail involved in each review. If the relevant initiatives listed in the Strategic Plan are subject to their own timelines and review processes, it may not be necessary to review all aspects of the Strategic Plan in detail every year.

## Question 7: Other topics not covered in the plan

### The wild west of cryptocurrency desperately needs addressing

While the broader realm of cryptocurrency no doubt requires a more detailed framework for regulation (if this is the Government's plan) than simply treating it as a payment method, we were surprised by the absence of any plan or timeline in the Strategic Plan for intervention in the private cryptocurrency industry and market.

Since Treasury's consultation earlier in 2022 on its proposal to regulate CASSPrs, the risks of cryptocurrency have become even more pronounced, in terms of market manipulation, their nature as a highly speculative and risky investment product and as a platform for scammers to operate. Something needs to be done, and quickly. We recognise that Treasury has recently released a consultation on token mapping of the industry, and there have been some recent comments about a more proactive intervention than was proposed in the early 2022 consultation. We support this and consider that there clearly to be a case for significant intervention in the sector.

Scamwatch reported that 2021 saw crypto increasingly become a more common payment platform used by scammers,<sup>30</sup> and it is a trend we are seeing in our casework. This reflects the fact that our casework suggests the efforts of these platforms to protect their customers from scammers is minimal.

We reiterate our urgent recommendations above that the banks need to do more to prevent scams from occurring on their platforms. However, scammers will go where it is easiest to access money. If banks improve their standards in scam prevention, there would be a desperate need to bring CASSPrs (and any other relevant entities) along with them, to ensure that the wider payments system is safe.

**RECOMMENDATION 7.** Any obligations imposed upon banks to take steps to protect their customers from scams (or to reimburse them for losses not prevented) should be replicated and mandatory for any entities operating in the cryptocurrency space, such as CASSPrs.

---

<sup>30</sup> <https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf>

## Further information

Please contact Policy Officer **Tom Abourizk** at **Consumer Action Law Centre** on [REDACTED] or at [REDACTED] if you have any questions about this submission.

Yours Sincerely,

**CONSUMER ACTION LAW CENTRE**  
**FINANCIAL RIGHTS LEGAL CENTRE**



## APPENDIX A - LIST OF RECOMMENDATIONS

- RECOMMENDATION 1.** Add 'fairness' as an additional key principle to guide the future of the payments system.
- RECOMMENDATION 2.** The Strategic Plan should recognise recent trends that indicate the payments system is most in need of interventions targeting improvements to its safety and security in the medium term.
- RECOMMENDATION 3.** As part of its initiatives addressing scams and fraud, the Strategic Plan should provide a framework for consulting on and introducing obligations for firms (including banks, super funds and CASSPrs) to detect and prevent scams on their payment systems. These obligations should impose financial responsibility for scam losses on system providers where relevant standards are not met.
- RECOMMENDATION 4.** The Government should use the Strategic Plan to set a timeline for mandating that banks introduce confirmation of payee technology, or otherwise provide customers with the ability to check the account name of a transfer recipient matches their intended recipient.
- RECOMMENDATION 5.** Treasury and the Government, in conjunction with the ACCC and AFCX, should explore ways in which the sharing (and use) of real-time transaction data on scams between banks can be mandated and fasttracked. This should be an initiative in the Strategic Plan.
- RECOMMENDATION 6.** The Strategic Plan should include pathways to resolving the issues that prevent people from cancelling recurring payments set up via cards, as a priority.
- RECOMMENDATION 7.** Any obligations imposed upon banks to take steps to protect their customers from scams (or to reimburse them for losses not prevented) should be replicated and mandatory for any entities operating in the cryptocurrency space, such as CASSPrs.

## **APPENDIX B – ABOUT OUR ORGANISATIONS**

### **Consumer Action Law Centre**

Consumer Action 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.

### **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 is an operator of the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.