Scams – Mandatory Industry Codes

Submission to Treasury Consultation Paper

January 2024

afca
Australian Financial Complaints Authority

Contents

Introduction

Scams are ubiquitous, increasingly sophisticated and constantly evolving. Even while the public discourse about and general awareness of scams across the Australian community has grown, financial losses continue to balloon. Scammers, often international organised crime syndicates, have taken advantage of the rapid move to the digitisation of products and services, including in banking, harnessing the benefits of friction-free, fast transactions and online/mobile payments. With innovation comes new risks and scams have exposed weaknesses in the risk management of social media platforms, telcos and financial firms, together with a lack of clarity about respective responsibilities to identify, deter, disrupt and remedy scam activity.

Australian consumers lost at least $3.1 billion to scams in 2022, which represented an 80% increase on total losses recorded in 2021[1]. Scams with a financial component reported to Scamwatch in 2023 increased almost 10%[2] and in the calendar year 2023, AFCA registered 8,987 scam related complaints, which was an increase of 95% from 2022. Consumers who fall victim to scams suffer both financially and emotionally and outcomes can be devastating.

As the single external dispute resolution (EDR) scheme for the financial services industry, AFCA plays an important role in the consumer protection framework. All licensed retail financial firms including Australian banks and Authorised Deposit Institutions (ADIs) are members of AFCA, and we have significant experience[3] in seeking to resolve complaints by consumers who have been affected by scams. As the financial services EDR scheme, our submission necessarily focuses on the ADI sector.

It is timely and appropriate the Government is taking action to shift the dial on scam detection, disruption and redress, including the establishment of the National Anti-Scam Centre (NASC) which draws on expertise from the private sector, consumer groups and other regulators to disrupt scams before they reach consumers.

AFCA recognises that more measures need to be implemented to protect consumers from scam conduct and to provide them with effective avenues for redress if impacted by a scam. We therefore welcome Government's Scams – Mandatory Industry Codes Consultation paper (the consultation paper) and the opportunity it presents to establish a universal framework that is consumer-centred and effectively provides redress when things go wrong.

[1] ACCC Targeting scams
[2] Scam statistics | Scamwatch
[3] AFCA and its predecessor schemes – Financial Ombudsman Service, Credit Industry Ombudsman and Superannuation Complaints Tribunal

Executive Summary

In the three-year period from 1 January 2021 to 31 December 2023, AFCA received 17,331 scam-related complaints. Our data shows that we have received a steady increase in monthly scam complaints since January 2021 (n=215) to December 2023 (n=740), with a peak of 1,077 monthly complaints received in August 2023[4]. This increase accords with reports to Scamwatch over the same period. While AFCA is receiving more complaints on average each month, the average financial loss complained about has decreased over time. The average financial loss claimed over the three-year period was $31,333.

Most Australians never recover the money they have lost to a scam. The scams generating the highest aggregate losses are investment scams, where the consumer intends to make the payment to a third party, believing it to be a legitimate investment.

A recent report by the Australian Securities and Investments Commission (ASIC) about the scam prevention, detection and responses by the four major Australian banks[5] said that bank customers are overwhelmingly the bearer of scam losses. Of the top 10 firms that AFCA receives scam complaints about (who are all ADIs), the highest average claimed scam losses returned to consumers was 35%.

About 58% of scam related complaints received by AFCA over the three-year period were closed at our Registration and Referral stage. This is the first stage of the AFCA process where member firms can resolve complaints directly before they move into active case management and investigation.

While AFCA encourages financial firms to resolve as many complaints as possible at this stage, we generally do not receive or record information about the outcomes of these complaints, as this information is dependent on parties notifying AFCA of the value of the outcome they reached. This highlights the need for ecosystem-wide reporting and transparency to fully assess:

- scams incidence and the numbers of scam related complaints made to firms (and outcomes) at internal dispute resolution (IDR)
- comparison of how firms within and across sectors are responding to prevent, detect and disrupt consumer losses
- the effectiveness of the Codes framework implemented out of these reforms.

AFCA strongly supports consistent measures to disrupt and prevent scams as a first line of defence. However, where consumers suffer losses because scammers

[4] Total scam complaints received, including those complaints closed at our initial stage of Registration & Referral
[5] ASIC Report 761

continue to breach these defences, then effective dispute resolution relies on accessibility and clear articulation of firm obligations and industry conduct standards.

As the consultation paper acknowledges, the current liability framework for banks and ADIs provides different outcomes depending on whether a scam is considered to be authorised or unauthorised (or where the underlying conduct is considered to be fraudulent). It also excludes, in the banking sector, consideration of the role of receiving banks in scam transactions.

In our view the new Framework should comprehensively cover all types of scams and that Codes for all sectors should set meaningful standards that provide a clear pathway for assessing and allocating liability including between each sector. As the framework is currently presented, it does not do this.

Our submission

In our submission, we provide a breakdown of the top 10 financial firms that AFCA received scam complaints about and the subsequent complaint outcomes. We also highlight the firms which will not be caught by the proposed Scam Code Framework (the Framework) but feature in our top 25 list of scam related complaints by volume.

Approximately 6.7% of scam complaints received in the past three calendar years that progressed to case management were resolved by formal determination by an Ombudsman or Panel. These complaints tend to be more complex or involve higher losses.

As a result of our review of cases that progress to determination, and our extensive case management experience, AFCA's submission highlights what we consider are the main opportunities, gaps and limitations of the current regulatory and legal framework as well as the inconsistent outcomes that scam victims often receive from financial firms when they complain. In many cases this inconsistency is inexplicable to consumers who have suffered the loss.

We acknowledge the Scam-Safe Accord[6] (the Accord), as announced by the Australian Banking Association (ABA) in November 2023, between Australia's community owned banks, building societies, credit unions and commercial banks and its set of anti-scam measures to be implemented across the industry. We also acknowledge announcements by individual banks about various initiatives seeking to make banking safer for their customers.

While the Accord and other initiatives are welcome and positive commitments that will be implemented at various stages, the development of the Framework provides an opportunity to raise standards consistently across all sectors in a timely way. Importantly, the Accord does not deal with liability for scam complaints.

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

AFCA is calling for a consumer centric model that provides:

- Adequacy of resourcing by firms to respond to and monitor scams and putting the onus on financial and other firms in the ecosystem to design products and services that minimise the risk of abuse by scammers.
- Strong outcomes-based obligations in the Codes and provision for public reporting against these obligations (including when they are not met by a Code participant).
- Consideration of timely introduction and expansion to other sectors including superannuation and digital asset platforms to manage the risk that scam losses migrate to lesser regulated sectors.
- The ability of regulators including ASIC and the Australian Competition and Consumer Commission (ACCC) to take effective and timely regulatory action for breaches of both principles-based obligations and sector specific Code standards (e.g. with appropriate penalties) and minimising regulatory duplication and uncertainty of roles.
- Clear (and stronger) rules/principles around liability for scam complaints including both "authorised" and "unauthorised" transactions and consideration of whether these distinctions are still appropriate and workable.
- A dispute resolution framework for scams complaints that leverages existing EDR scheme capability and expertise and makes it as easy as possible for consumers to make complaints and achieve fair outcomes.
- Clarity about how liability will be allocated within and across sectors when a breach of Code standards (or the law) has caused/contributed to consumer losses. This is essential for effective dispute resolution.
- Prompt review and expansion of the ePayments Code (as set out in the *Payments system modernisation: regulation of payments service providers consultation paper*) noting earlier comments about the treatment of unauthorised/authorised transactions and extending protections to small business customers.

The Government's stated objective for the Framework is that *"These tough new Codes would make it really clear what the obligations are on industry to prevent scams and better protect people and businesses."* AFCA's submission is particularly shaped by this objective.

A key success measure for the Framework will be its ability to drive consistent effective action by businesses. AFCA has therefore also identified five key initiatives in this submission that would, based on our complaints experience, assist in reducing scam incidence and losses.

About AFCA

AFCA is the EDR scheme authorised under the *Corporations Act 2001* (Corporations Act) to deal with complaints about all licensed firms in the financial sector including banks and other ADIs.

The AFCA scheme is overseen by ASIC and is required by legislation to operate in a way that is accessible, independent, fair, accountable, efficient and effective. AFCA resolves complaints that individual or small business consumers make about their financial firms. Our complaint resolution service, provided free to consumers, is an alternative forum to tribunals and courts, and in most cases our decisions are binding on financial firm members, if accepted by the complainant.

Our scheme operates under the AFCA Rules (Rules) which set out the rules and processes that apply to all complaints submitted to AFCA, including superannuation complaints. This includes what complaints we can consider, the procedures we can use to resolve them, remedies we can provide and related matters including our reporting obligations.

When determining complaints, the AFCA decision maker must do what is fair in all the circumstances, and have regard to:

- legal principles
- applicable industry Codes or guidance
- good industry practice
- previous relevant determinations of AFCA or predecessor schemes[7].

AFCA also publishes detailed Operational Guidelines which explain in more detail how we will interpret and apply our Rules when considering complaints involving financial firms.

In addition to providing solutions for individual financial complaints, AFCA has responsibilities to identify, resolve and report on systemic issues and to notify ASIC, and other regulators, of serious contraventions of the law. AFCA works closely with ASIC and regularly liaises with it to share complaint insights, to inform and assist its regulatory work. Further, AFCA's Code Team supports independent committees to monitor compliance with Codes of practice in the Australian financial services industry, and to achieve service standards that people can trust.

More broadly, AFCA plays a key role in restoring trust in the financial services sector. Since its establishment on 1 November 2018, AFCA has handled over 367,000 complaints and delivered over $1.07 billion in compensation to consumers. Our systemic issues work has resulted in 4.8 million people receiving more than $340 million.

[7] AFCA Rule A.14.2

AFCA Scams data and insights

This part of our submission contains data and analysis about the scam complaints AFCA has received. Unless expressed otherwise, the data is shown for the period 1 January - 31 December 2023. Before this, AFCA did not systematically apply scam flags to our complaint records.

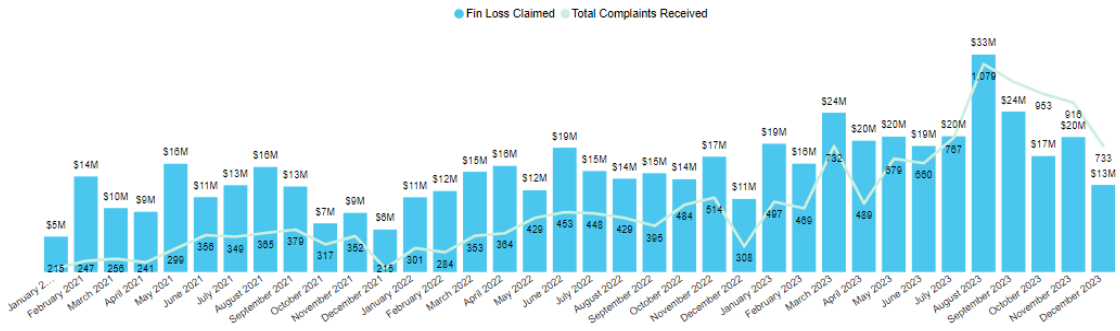
AFCA has received 17,331 scam complaints in the three year-period. Annual calendar year statistics are shown below in Chart 1, along with statistics on the number of complaints that progressed further than our initial Registration and Referral stage to Case Management. A comparison of month-on-month variations in scam financial loss reports to Scamwatch and AFCA since 2021 suggests that there is a positive correlation between reporting volumes at both AFCA and Scamwatch, although we note that the average reported loss per scam case received in the past 12 months is significantly higher at AFCA than with Scamwatch ($32K vs $16.5K).

Chart 1: Scam complaints received in calendar years 2021-2023

Year	Complaints received	Complaints accepted
2021	3,591	1719
2022	4,762	2114
2023	8,978	3530
Total	17,331	7363

Chart 2[8] provides a monthly breakdown of total scam complaints lodged with AFCA in the three-year period 1 January 2021 – 31 December 2023. The chart also shows monthly changes in financial losses claimed through these complaints.

Chart 2: Scam complaints and financial losses claimed by month



Whilst overall complaint volumes and aggregated losses have been increasing, the average financial loss claimed per complaint has steadily reduced (due to the accelerating number of small value claims being made to AFCA). While this is the

[8] Chart 1.1 does not include complaints where the compensation claimed exceeded compensation limits in AFCA's Rules.

case, we continue to see many scam complaints where claimed losses exceed $100K.

Chart 3: Total Scam Complaints and Average Fin Losses Claimed per Case

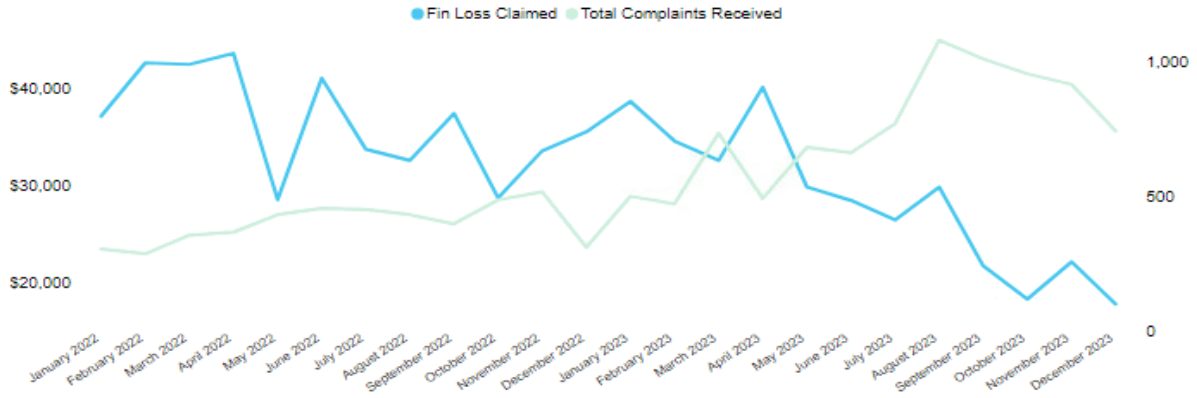


Chart 4 shows the top 10 financial firms that AFCA has received scam complaints about over the three-year period. It includes total numbers of complaints received and the total losses **claimed** by customers who made these complaints Unsurprisingly, this chart features some of the largest bank and ADI members of AFCA and scams complaints incidence can be expected to correlate with business size.

Chart 4: Top 10 financial firms who had scam complaints lodged with AFCA

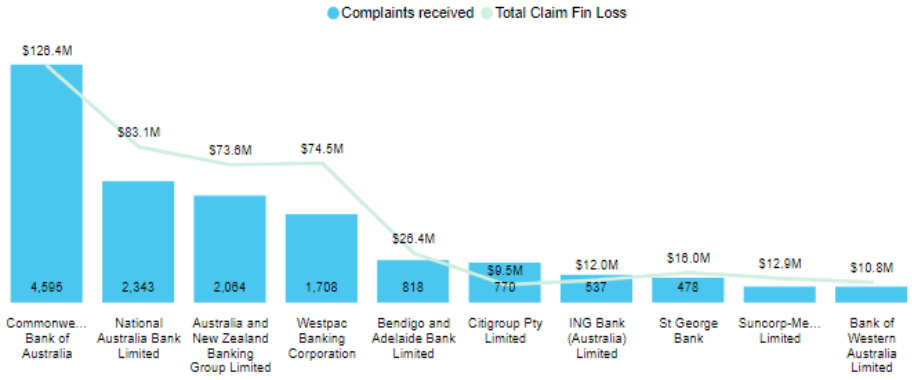


Chart 5 is an expanded list of the top 25 financial firms that AFCA has received complaints about over the three-year period. We have provided this to show the larger cohort of financial firms that receive scam complaints and to highlight firms that are captured in this list but will be outside the scope of the proposed scams Framework. The columns in this table show:

- Total number of scam complaints received by firm and the financial loss **claimed** by consumers when lodging their complaints.

- The proportion of these complaints that were then **accepted** by AFCA. This means cases that were not resolved by firms at our initial Registration and Referral stage and so have progressed into active case management by AFCA.
- The total financial loss claimed by consumers in relation to these accepted complaints; and finally
- The average outcome rate for closed cases which is a measure of the percentage of claimed losses by consumers that was returned to them at the conclusion of the AFCA dispute resolution process.

As Chart 5 shows, the average outcome rates across all 25 firms for the three-year period ranges from 6% to 40%.

Chart 5: Top 25 financial firms who had scam complaints lodged with AFCA[9]

MemberName	Complaints received	Claimed Fin Loss	Complaints accepted	% Accepted	Claimed Fin Loss (Accepted)	Complaints closed	Avg of Outcome Rate % (accepted/closed)
Commonwealth Bank of Australia	4,596	$125.7M	1460	32%	$74.4M	4,223	17%
National Australia Bank Limited	2,343	$83.1M	900	38%	$56.3M	2,210	13%
Westpac Banking Corporation	1,707	$74.5M	773	45%	$54.4M	1,622	13%
Australia and New Zealand Banking Group Limited	2,064	$73.6M	786	38%	$46.5M	1,951	9%
Bendigo and Adelaide Bank Limited	820	$26.4M	535	65%	$18.5M	668	13%
St George Bank	478	$16.0M	177	37%	$12.4M	459	11%
Suncorp-Metway Limited	308	$12.9M	159	52%	$8.4M	285	16%
ING Bank (Australia) Limited	538	$12.0M	362	67%	$9.5M	493	15%
Bank of Western Australia Limited	305	$10.8M	175	57%	$6.5M	286	16%
HSBC Bank Australia Limited	302	$10.2M	225	75%	$6.2M	206	19%
Citigroup Pty Limited	771	$9.5M	258	33%	$7.6M	739	40%
Macquarie Bank Limited	285	$8.2M	191	67%	$5.2M	233	20%
Casey Block Services	108	$7.3M	74	69%	$5.3M	100	7%
Bank of Melbourne	149	$6.5M	67	45%	$4.9M	143	24%
Bank of Queensland Limited	132	$3.8M	87	66%	$3.0M	115	10%
Wise Australia Pty Ltd	76	$3.1M	66	87%	$2.4M	57	6%
PayPal Australia Pty Limited	198	$2.6M	64	32%	$2.3M	184	26%
BankSA (a division of Westpac Banking Corporation)	96	$2.5M	37	39%	$1.6M	92	16%
Beyond Bank Australia Limited	123	$2.5M	72	59%	$1.9M	110	24%
Heritage and People's Choice Limited	119	$1.7M	88	74%	$0.9M	86	19%
Great Southern Bank	115	$1.4M	59	51%	$1.2M	103	17%
Members Equity Bank Limited	119	$1.4M	47	39%	$0.8M	114	22%
Newcastle Greater Mutual Group Ltd	74	$1.3M	56	76%	$1.0M	62	13%
Latitude Finance Australia	95	$0.6M	27	28%	$0.3M	86	20%
American Express Australia Limited	163	$0.3M	24	15%	$0.2M	158	29%
Total	16,084	$497.8M	6769	42%	$332.0M	14,785	15%

Chart 6 shows the stage in which the scam complaint closed. Approximately 61% of scam complaints closed in the last three years resolved at our initial stage of Registration and Referral, 29% of scam complaints resolved in case management and 7% following a Rules review (review of AFCA's jurisdiction) and 3.5% of all scam complaints proceed to a decision[10].

[9] For completeness, this Chart does not include outcome rates of the total complaints received because we cannot quantify actual outcomes for complaints closed at Registration and Referral.
[10] To clarify varying statistics on the number of scam complaints that progress to a Decision – 3.5% represents the percentage of all scam complaints that progress to a Decision. 6.7% represents the percentage of scam complaints that progress to a Decision, only accounting for scam complaints that are accepted (i.e. of complaints that progress to Case Management).

Chart 6: Resolution Stage of scam complaints (cases closed 3 years to Dec 23)

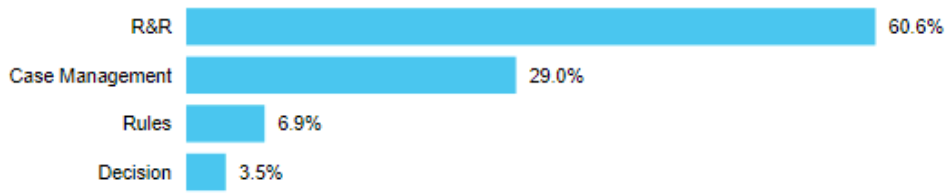
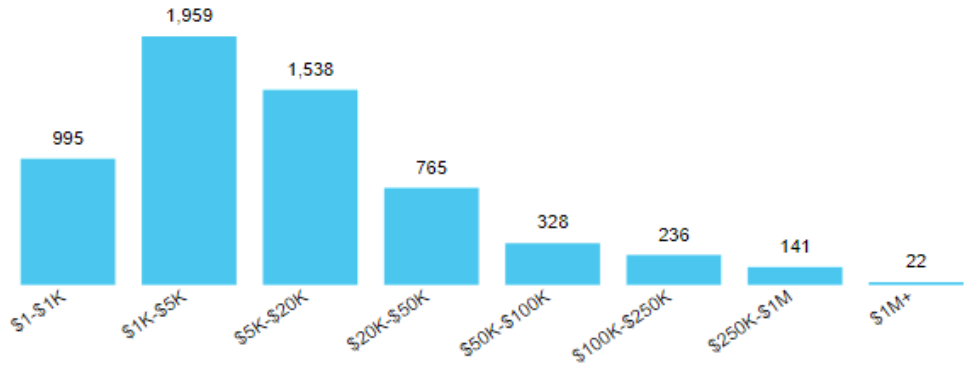


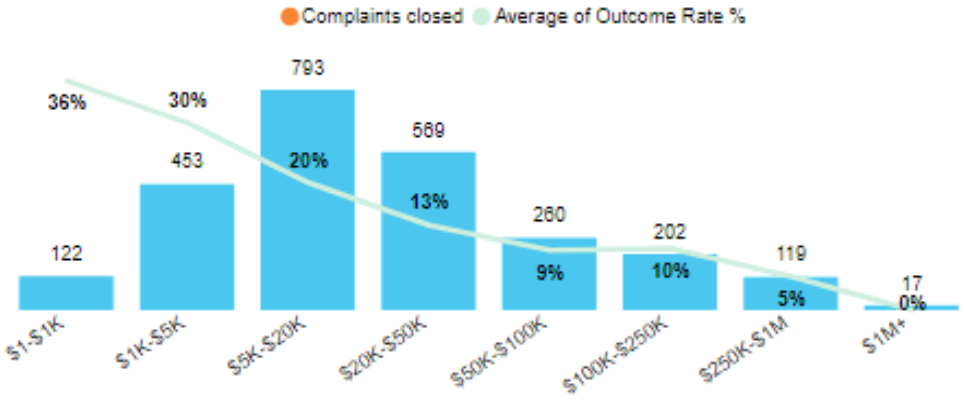
Chart 7 shows the distribution of losses claimed in all scam complaints that were closed by AFCA in the past 12 months. This includes all complaints closed at Registration and Referral[11].

Chart 7: Distribution of financial loss in complaints made to AFCA



For the smaller subset of scam complaints that were accepted into case management and closed by AFCA in the past 12 months, Chart 8 shows the average outcome rate for complaints relative to the financial loss claimed by the consumer[12]. It shows that complaints with lower value claims tend to receive higher outcomes.

Chart 8: Average outcomes by accepted complaints based on losses claimed



[11] Chart 7 excludes complaints against which no financial loss was recorded.
[12] Chart 8 excludes complaints against which no financial loss was recorded.

Current limits on AFCA's ability to resolve scam complaints

AFCA must consider and resolve complaints according to our Rules. We have described above our decision-making test, which relies heavily on the application of existing law and Codes to the individual facts the subject of the complaint. In this and the following section we set out some of the limitations in AFCA's Rules and gaps in the law and industry Codes that affect how we currently resolve scam complaints.

AFCA believes these current limitations should be considered by Treasury and where appropriate, addressed in the next iteration of the Framework.

Limits on AFCA's jurisdiction in dealing with scam complaints

There are a range of jurisdictional limits that can affect AFCA's ability to deal with the full range of scam complaints that are lodged with us. For example, we do not have jurisdiction to look at the actions of a receiving bank in a scam transaction. This includes where the receiving bank's processes may have facilitated the opening of a mule account to enable the scam.

In comparison, the UK Financial Ombudsman Service can look at the conduct of the receiving bank as a result of a change in its rules in January 2019. Importantly, these changes were supported by the introduction of a Contingent Reimbursement Model (CRM) Code[13] which explicitly provides that a receiving bank should share liability with the sending banking in certain circumstances.

AFCA also cannot generally consider complaints where an account is opened using stolen identification documents. This is because the person impacted did not receive a financial service or does not have a customer relationship with the relevant bank, which is necessary to satisfy the eligibility criteria under the AFCA Rules.

AFCA can also only consider complaints about financial firms that are members of the scheme. Most firms dealing with retail consumers in the financial system are required to have AFCA membership through ASIC licensing, however there are currently some clear gaps in the scams ecosystem, particularly crypto platforms and providers.

Compensation caps

AFCA operates under monetary and compensation caps. These limits are indexed every 3 years, and for complaints lodged after 1 January 2024 the compensation claim limit increased from $542,500 to $631,500 while the monetary claim limit increased from $1,085,000 to $1,263,000. For complaints lodged on or after 1 January 2024, AFCA can also award a maximum of $6,300 per claim for non-financial and indirect loss.

[13] https://www.lendingstandardsboard.org.uk/crm-Code/

These limits are adequate for most scam complaints AFCA receives. Over the three-year period to 31 December 2023, we closed a limited number of complaints (17) because they were over AFCA's monetary caps[14]. We note AFCA's compensation jurisdiction is significantly higher than the Telecommunications Industry Ombudsman (TIO). There are still however a small number of complaints that fall outside the jurisdiction.

Limits in the law and industry Codes

Assessing liability in scams complaints is complex, highly contextual and typically requires an assessment of whether a transaction is authorised or unauthorised.

Under the current laws and codes a consumer can usually only succeed in a claim for compensation where they have not made the transaction themselves or had someone make it on their behalf (so it is unauthorised) and have not voluntarily disclosed the majority of the passcodes required to perform the transaction.

Where the payment is authorised the consumer will not usually succeed unless the bank has done something wrong.

If the person who was scammed is a consumer (e.g. rather than a small business) and if the relevant bank (from where the monies were taken/withdrawn) is a subscriber to the ePayments Code (ePC), then we can consider whether the liability provisions of the ePC assist in determining the complaint.

Scope of the ePayments Code

The ePC is a voluntary industry Code that superseded the Electronic Funds Transfer Code in 2011. According to ASIC's website, '*Most banks, credit unions and building societies currently subscribe … along with a number of non-banking businesses'.* It applies to consumers where a transaction to which the ePC applies (electronic and telephone) is performed wholly or predominately for personal domestic or household purposes. The ePC does not provide cover for transactions by individuals using a facility designed primarily for use by a business and established primarily for business purposes[15].

Our cases show that there are in practice limited avenues for recovery in a scams complaint under the ePC, given the current definition of *unauthorised transactions*. The ePC that took effect on 2 June 2023 clarified the definition of unauthorised transaction as one that is not made by the customer or with their knowledge and consent.

This definition means that payments made by a person or by the scammer with the customer's knowledge are treated as authorised payments even though the customer

[14] Some caution should be taken with this data as it is possible that there may have been more complaints that were outside AFCA's monetary limits but where the consumer did not attempt registration at AFCA.
[15] Although in some circumstances, the terms and conditions of the business account may extend the application of the ePC to determine liability for unauthorised transactions

did not intend to pay (or was tricked into paying) a scammer or a mule account. When finalising its review of the ePC in early 2022, ASIC acknowledged that the ePC was not intended to cover scams. In its current form the ePC also does not consider technology such as tokenisation and digital cards/wallets.

The ePC does, however, provide a regime to determine liability for unauthorised transactions and so if a scam transaction falls within the definition of "unauthorised" then the ePC is relevant to determine whether the firm, or the customer, should be liable for the loss.

It is important to note that consumers who have lost money will typically describe the scam transactions as "unauthorised" when they are making a complaint. This is because they do not feel they have authorised the payment to a scammer but have done so by mistake or under duress or because of misleading conduct. Whether a transaction is technically unauthorised under the ePC however, requires a specific analysis of the definition in the ePC and its application to the circumstances of the transaction (or series of transactions).

It is not clear whether the proposed framework will adopt the current definition of unauthorised transaction. Any change to this will impact the framework and how it interacts with the ePC and will require changes to the ePC.

AFCA has seen an evolution in the types of scams that are complained about. We have seen scammers adapting to find entryways into new products and technologies and we have seen significant growth in scam transactions where consumers are persuaded or tricked by scammers to authorise payments. Typically, "authorised scams" involve investment scams, romance scams and scams inducing consumers to conduct buy/sell transactions. Some authorised scams also involve unauthorised payments as the scam develops.

Following is a case study where AFCA determined a scams complaint in favour of a consumer. This complaint highlights the very specific circumstances which arose to give rise to a successful claim under the ePC.

Voluntary Disclosure of passcodes – Case number 932870

Background

The complainant fell victim to a bank impersonation scam. The complainant received a call from a private number claiming to be from the bank's fraud department notifying her of suspicious and unauthorised activity on her account. To ensure she was speaking to the real bank she hung up and dialled the bank number but was placed in a queue and was advised via automated message that there was a 45-minute wait to speak to the next available operator. Shortly after, she received a call from the bank's number, which she assumed to be the bank calling her back but was in fact the scammer. The scammer created a sense of

urgency and panic. He advised her she would receive several SMS Codes to verify her identity and to allow him to view the account. She verbally provided two passcodes to the scammer as requested.

The scammer used this information to gain access to the complainant's internet banking profile and:

- used the temporary password to reset the complainant's internet banking password
- added a new payee and made a $2,500 transfer (authenticated via one-time passcode (OTP))
- made two further transfers of $1,210 and $4,225 to the same payee (no further OTP required).

Outcome

AFCA found the bank was liable for the disputed transactions as the bank was unable to show the complainant contributed to her loss by breaching the passcode security requirements in clause 12 of the ePC.

Most significantly, AFCA found the complainant did not *voluntarily* disclose her passcodes. The relationship between a bank and a customer is a unique relationship of trust. Where the complainant held an honest and reasonable belief she was talking to her bank, the circumstances when viewed as a whole did not displace that belief and when her bank asked her to read back a passcode which it sent to her to protect her account, AFCA found she would have felt compelled to do so.

Relevant factors in the complainant's favour included:

- The scammer spoofed the bank's genuine phone number.
- The scammer's request to provide verbal Codes for identification was consistent with the expectations of pin disclosure for telephone banking set out in the bank's own terms and conditions.
- The bank's spoofing scam alerts were not proximate enough to the scam to displace the complainant's reasonable belief.
- The OTP was read in preview mode, so the full text of the accompanying SMS including a warning not to share was not visible to the complainant.

Significance

ASIC recognised, in its comments on the disclosure prohibition in report 718[16], that rather than creating specific exemptions from the prohibition, it expects AFCA will continue to consider matters of reasonableness and fairness in appropriate cases.

[16] ASIC Report 718, *Response to submissions on CP 341 Review of the ePayments Code: Further Consultation*

This determination is significant in its interpretation of that prohibition in clause 12 of the ePC. In cases of unauthorised transactions in bank spoofing, there will be circumstances where verbal disclosure of passcodes to a bank- impersonating scammer is not considered voluntary and will not be in breach of clause 12. This case is also significant in demonstrating how each scam case turns on its own facts and involves careful weighing up of the specific circumstances.

Authorised transactions: Legal limitations

Complainants who make authorised pay-anyone transactions generally have very limited basis for recovery under current law and Codes unless it can be shown the bank has done something wrong. The current legal position on ADI liability is unclear and there are several areas where there are no obligations on financial firms except for the general conduct obligations under section 912A of the Corporations Act and the Banking Code of Practice (BCOP).

There are also currently no:

- laws or Codes that cover recall obligations of ADIs, including timeframes (outside the limited Mistaken Internet Payments regime in the ePC (which is confined to mis-typing errors or the selection of the wrong account in a drop-down box).
- Specific requirements on ADIs to provide easy access to customers to report scams and seek help, to avoid excessive wait times that are reported in some of our complaints.
- Specific obligations on ADIs to share scam data (and in real time) including about mule accounts.

ASIC's Report 761, *Scam prevention, detection and response by the four major banks* (REP 761), found banks adopted 'inconsistent and generally narrow approaches to liability, reimbursement and compensation'[17] and that the bases on which a bank might consider liability in a particular case included:

- Contractual obligations
- Implied warranties
- AFCA's approaches to similar matters
- Conduct failures including warning the customer, exercising due care or skill, making reasonable inquiries when on notice of potential scam/fraud and failure to apply own policies or procedures.

ASIC found however that the banks were not consistent either internally or between each other, in taking all these grounds into account from case-to-case. This aligns with AFCA's experience and highlights the practical challenges in seeking to resolve complaints in the absence of clear liability rules or principles.

[17] Page 20

The following case study provides an example of a complaint determined by AFCA where the consumer was unsuccessful in establishing the bank should have done more to prevent them from being scammed. As noted, it shows that banks' obligations in these cases can be relatively easily met and also highlights gaps caused by the exclusion of crypto platforms from the licensing framework (and therefore AFCA membership).

Authorised Crypto Investment scam – Case number 933547

The complainants are a retired husband and wife (Mr and Mrs H) who were attempting to create an investment portfolio. Mr H had been diagnosed with cancer and was undergoing treatment. In response to marketing material viewed online, Mr H reached out to who he believed was a broker from a legitimate company (scammer). The broker instructed them to download remote access software and coached them on how to increase their daily account limits and purchase cryptocurrency in trading accounts in their own names.

Between November 2021 and June 2022, the complainants authorised a series of transactions totalling over $670,000 for cryptocurrency trading. The broker obtained remote access to the complainants' computer and transferred the funds from the trading accounts to various other digital wallets himself. In April 2022, the complainants' son discovered the trading investment was a scam and together with the complainants reported it to the bank. Mr H continued to make several disputed transactions in June 2022 after which electronic access to the account was revoked by the bank. The complainant said he was vulnerable and can't remember what he told the bank when he spoke to them during this time.

The bank says it provided appropriate warnings to Mr H about the nature of the disputed transactions, but once Mr H instructed it to proceed, the bank was obliged to follow his authorised instructions. It says it could not be certain the transactions were fraudulent. The bank also said the co8mplainants suffered no loss from the disputed transactions as the funds were transferred into cryptocurrency wallets in the complainants' names.

Outcome

The bank was able to show it made reasonable enquiries of the complainants when internal fraud alerts were triggered. The call recordings did not raise question of capacity nor did the complainant Mr H alert the bank to his circumstances of vulnerability. Regardless, as the funds were made into a cryptocurrency trading account in the complainants' names, the complainants could not show they suffered a loss from the bank's error. No compensation was payable.

Significance

The bank's obligation to make reasonable enquiries can be easily met. This is especially so where a person is coached into answering the bank's questions in a

way which appears to address any concerns of the bank about the legitimacy of the transactions. In cryptocurrency investment scams, where funds are moved from an Australian bank into a cryptocurrency wallet in the name of the complainant, it is difficult to show that loss was suffered as a result of the bank's error.

Issues and questions raised in the consultation paper

Key features of the Framework

The Framework incorporates an overarching regime that will be introduced into primary law, administered and enforced by the ACCC, and three sector specific Codes and standards. These Codes are to cover banks (regulated by ASIC), telecommunication providers (regulated by the Australian Communications and Media Authority (ACMA)) and digital communication platforms (also proposed to be regulated by ACMA). The consultation paper says there is scope for further sectors to be designated in the future by the relevant Minister.

In our view, the success of the proposed Framework will depend heavily on the overarching framework and the sector specific Codes setting clear and measurable standards that directly influence both firm behaviour and investment (money/time/resources) and significantly improve consumer outcomes. It is essential that the Codes set clear obligations and the consequences in terms of liability to customers if those obligations are not met. There also needs to be a consideration of how failure to meet obligations will be reflected in any liability sharing framework.

The relevant Framework legislation must be drafted to be capable of effective enforcement by the regulators. Where there is overlap in possible regulatory responsibility (for example, between ACCC and ASIC in relation to the proposed overarching standards for banks and existing obligations e.g. to act honestly, efficiently and fairly under the Corporations Act), it is essential that there is clarity about regulatory jurisdiction.

There should also be transparent reporting of outcomes against the standards and obligations to determine the effectiveness of the Framework over time. It should also be clear what impact the failure to meet regulatory requirements will have on claims by individual consumers.

AFCA (and its predecessor EDR schemes) has extensive experience in liaising with and reporting to ASIC, which has a statutory approval role for the AFCA scheme under the Corporations Act. AFCA also currently deals with scam related complaints about all the banks and ADIs that are proposed to be captured in the first iteration of the Framework.

What future sectors should be designated and brought under the framework?

AFCA supports prompt consideration of superannuation-related scams being brought under the framework given the volumes of retail funds held in the superannuation system and the importance of ensuring that superannuation funds also have in place scam strategies, procedures and rules commensurate with the risk. While the number of scam and unauthorised transaction complaints made to AFCA against superannuation funds is currently low, we are beginning to see instances of sophisticated scam activity affecting the superannuation industry.

We also note that digital asset platforms often play a gateway for scam transactions (especially through cryptocurrency), and we would like to see an industry Code apply to this sector (see AFCA's recent submission - AFCA Submissions).

Definitions

Proposed definition of scam under the Framework: A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.

The definition of scam under the proposed Framework needs to be functionally broad enough to cover current and potentially emerging scam typologies. It is also important that the definition supports certainty of enforcement by the relevant regulators, and that it drives appropriate and comprehensive data recording and collection by firms. We note that the ACCC currently defines a scam as:

> *A scam is a way of tricking people into handing over money or personal details.*

AFCA is not recommending a particular definition, but we note that the ACCC definition may avoid consideration of the need to establish dishonest intent.

We also agree that there is a need to consider and be explicit about the appropriate perimeter between fraud and scams, noting that in the banking context under the card scheme rules in particular there are separate liability frameworks for (certain) fraudulent transactions. The Framework should also clearly include protections for small business customers.

Proposed definition of a Bank under the Framework: *It is intended that the Framework would apply to a body corporate that is an Authorised Deposit Taking Institution (ADI) under section 9 of the Banking Act 1959. Adopting this definition would mean that the scope of the Framework would extend to small and large banks, building societies, credit unions, and restricted ADIs.*

All of these firms are already subject to comprehensive IDR and EDR requirements through ASIC licensing and membership of AFCA.

We have provided a list of the top 25 financial firms represented by scam complaint numbers made to AFCA (see pg. 7). Analysis of these figures show that there are four firms in this list that would fall outside the initial scope of the Framework. They are Casey Block Services (trading as CoinSpot), Wise Australia, Paypal and Latitude Financial.

Principles-based obligations

The consultation paper states that:

*It is intended that the CCA would set out **clear and enforceable** principles-based obligations. These obligations would require all businesses subject to the Framework to take a consistently proactive approach to combatting scams, irrespective of the sector in which they operate*[18] (emphasis added).

The proposed ecosystem-wide obligations in the CCA are set out on page 12 of the consultation paper. We highlight below some issues that could be considered when settling these obligations and that are aligned with questions 15-19 of the consultation paper:

- There should be express rules around adequacy of resourcing. ASIC Report 761 found that for three of the banks reviewed, information indicated that their staff resourcing levels and capability had not kept pace with the increasing volume and sophistication of scams.
  - > AFCA also sees complaints where consumers report unacceptable wait times to report a scam or speak to bank staff or where scam centres are closed. We have also seen resourcing variances where one firm had staff available on Christmas Day while another had no one available to take a scam-related call on a weekend.
  - > Scams occur 24/7 and therefore scam centres/avenues to report and act on scams should be available on the same basis.
- Products and services (across the scams ecosystem) should be designed to minimise likelihood of scam abuse.
- The introduction of public reporting and regulatory reporting about scams losses and amounts recovered by consumers/small businesses including through complaints processes would add transparency and accountability to the Framework
- It is important that the provisions are practically enforceable and have adequate penalties under the CCA for non-compliance. It will also be important to clarify how breaches of these obligations will flow into considerations of consumer compensation.

[18] Consultation Paper, p.11

We note that ASIC Report 761 also found that there was room for improvement in reporting to Boards about scams and committing to internal and/or external audits of the effectiveness of the anti-scam strategy. These are practical measures which may be appropriate to build into the proposed ecosystem-wide obligations.

Anti-scam strategy

Under the proposed Framework, businesses would be required to *develop, maintain and implement an anti-scam strategy that sets out the business' approach to scam prevention, detection, disruption and response, based on its assessment of its risk in the scams ecosystem*. The consultation paper says that this would be subject to review by the ACCC which also could *play a role in working with businesses on their anti-scam strategies to ensure they are fit-for-purpose and consistent with similar businesses in their sector* (p.13).

As currently drafted, we think that this obligation sets out what could be described as basic hygiene for a retail business dealing with customer money/payments, notwithstanding that ASIC report 761 found that only one of the major banks had:

- a documented bank-wide scams strategy in place at the time of that review (conducted between May 2022 and February 2023); and
- undertaken a review of its scam prevention activities to ensure they remain fit for purpose, during the previous 3 years.

ASIC has said that it would be monitoring the actions taken by the major banks in response to the findings in Report 761 and that it had commenced a review of the scam measures in place in other parts of the banking industry. This is important work that will need to continue to take place when the proposed scams Framework is in place.

We endorse a Framework that explicitly sets out what monitoring is to be done and by which regulator. Regulators will need to be adequately resourced to undertake this work effectively to ensure that there is broad public confidence in the Framework and to minimise the numbers of complaints coming through to EDR schemes including AFCA. The Framework should also set out the consequences that apply if a firm does not have an adequate scams strategy.

Information Sharing and reporting requirements.

We agree with the commentary in the consultation paper about the critical importance of keeping records of incidences of scams and sharing data and information on these incidences across the ecosystem. Information needs to be shared in real time so that firms can take appropriate action to stop losses through steps including blocking transactions and accounts. This would need to be facilitated by 24/7 access to any data and information sharing and service standards to ensure information is shared quickly to enable appropriate responses.

AFCA supports the investment by the major banks in the Australian Financial Crimes Exchange (AFCX) to date. While AFCA does not have access to this platform, our general approach in determining complaints is that if the scam entity is, for example, listed on Scamwatch then the ADI should have known and taken appropriate action to stop or block consumer transactions and will be held liable when this does not happen. We will continue to apply this approach as reporting and information sharing is expanded.

Consumer reports, complaints handling and dispute resolution

One of the stated objectives of the proposed Framework is that:

> *Where a business does not meet its obligations under the Framework, where applicable, Internal and/or External Dispute Resolution mechanisms would ensure consumers have access to* ***appropriate redress****, and regulators would be given new enforcement and penalty powers*[19] (emphasis added).

Before we turn to the issues identified in questions 30-33, it is useful to consider how appropriate redress will be delivered in a complex, multi-party framework as proposed in the consultation paper.

As reflected in our data, Australians are making scam complaints in increasing numbers. While AFCA is seeing a higher incidence of smaller value claims through its case work (relatively more of which are settled by firms directly) cases that progress through to decision are increasingly complex.

Consumers should be at the centre of the design of the dispute resolution framework for scams. We agree that the Framework should continue to support the longstanding dual IDR and EDR resolution stages. It should also be clear and simple for consumers to escalate a complaint to one EDR scheme, even where there may be multiple firms potentially from different sectors that ultimately share liability.

Multiple EDR schemes were a feature of the financial services dispute resolution framework prior to 2018. We point to the final report of the *Review of the financial system external dispute resolution and complaints framework* (3 April 2017) which recommended the establishment of a single EDR scheme for the financial sector – AFCA – primarily on the basis that multiple schemes lead to:

- increased risk of consumer confusion
- increased risk of inconsistent outcomes for consumers
- duplicative costs for industry and for regulators which are overseeing those schemes[20].

[19] Consultation paper, p.6
[20] Pg. 109 Final Report - Review of the financial system external dispute resolution and complaints framework (Ramsay Review Final Report)

AFCA therefore supports a single-entry point for consumers who are escalating scam complaints. To date, most consumers making scam complaints "follow the money" – meaning that their first point of complaint tends to be the particular bank, ADI, payments provider or crypto platform from where their monies were withdrawn/transferred or "lost". Similarly, through NASC, the major banks, other businesses and governments are brought together to fight against financial and cyber-crime in Australia.

A further prerequisite for ensuring appropriate redress is a clear articulation of liability for losses arising from scam complaints and, if there are to be multiple parties (within and across sectors) that might share liability in a particular case, clarity about how liability will be allocated. This is necessary for both IDR and EDR to operate efficiently and to drive fair and consistent outcomes for consumers.

We think more work needs to be done on this issue. AFCA notes for reference that the Monetary Authority of Singapore has recently consulted on a proposed Shared Responsibility Framework[21] for scam losses amongst financial institutions (FIs), telecommunication operators (Telcos) and consumers, for unauthorised transactions arising from phishing scams. Under these proposals FIs and Telcos will provide payouts to scam victims for a defined set of phishing scams, if specified anti-scam duties are breached, with FIs proposed to stand "first in line" as custodians of consumers' money.

Limitations and gaps in leveraging existing IDR requirements and EDR schemes

The consultation paper contains a high-level discussion about complaints handling and dispute resolution. AFCA supports the extension of key standards contained in RG 271 across each of the sectors captured by the Framework. RG 271 is comprehensive, outcomes-oriented and has been implemented by financial firms since October 2021. It is also based on Australian Standard AS/NZS 10002:2014, *Guidelines for complaint management in organisations* which was developed as an economy-wide complaints handling standard. If the Framework is going to achieve its intended objectives of setting consistently high standards, this would be a good place to start, noting that most complaints about scams are dealt with by firms internally at first instance.

EDR arrangements for financial firms and telecommunication providers have been in place for decades through the operation of AFCA (and its predecessor schemes) and the TIO. It will be important that Government identify how EDR complaints about digital platform providers will be determined.

As previously noted, AFCA is required to identify and report systemic issues, serious contraventions of the law, and other reportable matters, to regulators including ASIC,

[21] Monetary Authority of Singapore - Consultation Paper

the Australian Prudential Regulation Authority and the Australian Taxation Office[22]. When the Framework is in place, AFCA may identify, through its dispute resolution work, breaches or systemic failings of requirements set out in either the principles-based obligations or the sector specific Codes and standards. To ensure effective oversight, it would therefore be appropriate for AFCA to also be able to report to the ACCC and potentially to ACMA where these regulators are responsible for the underlying conduct. This would require law reform.

Apportionment of liability and referral between EDR schemes

As noted above, if there are to be multiple parties to a scams complaint, then clarity about apportionment of liability is critical for ensuring that appropriate redress is delivered under the Framework. We think that the sector specific Codes are likely to be the right place for specific conduct and liability standards to be housed.

Under its Rules[23] AFCA can join another financial firm as a party to a complaint at any time that we decide it is appropriate. The financial firm must be a current member of AFCA for us to do this. When we are considering complaints involving multiple parties we will assess:

- Each firm's conduct and whether it breached any legal or other obligations
- Whether any identified breaches caused the consumer loss; and
- Whether the consumer should be awarded compensation for the claimed loss. In any complaint, including scam complaints, AFCA will also have regard to the complainant's conduct and any contribution they made to the loss.

Government may wish to consider AFCA's approach to apportionment if developing liability settings where multiple firms are involved.

Compensation caps and pathway to compensation

For some of the reasons discussed in this submission, the Framework does not currently set out a **clear pathway** for compensation (q.33) but we agree that this is the right question to be posed when drafting and settling standards and obligations. AFCA deals with all complaints on their individual merits, and our experience has been that financial firm liability can turn on very specific details when applying existing law or Codes.

The consultation paper asks whether compensation caps should be harmonised at EDR across sectors. AFCA would not support any reduction in its monetary and compensation limits which are contained in our Rules and subject to indexation every 3 years.

[22] Section 1052E Corporations Act 2001
[23] Rule A.6

Sector-specific Codes and standards

As noted earlier in relation to the principles-based obligations, the standards set out in the sector specific Codes need to be specific and measurable, to ensure that stakeholders and Government can assess actual outcomes against specific criteria, and so that they can be applied effectively in a dispute resolution context.

While AFCA notes the consultation paper's reference to telecommunications providers being the only sector specifically regulated in relation to scams under the *Reducing Scam Calls and Scam Short Messages Code* (SCSSM Code), this Code does not appear to have any powers and sanctions to address Code breaches. AFCA strongly supports the inclusion of powers and sanctions in the relevant scam industry Codes contemplated under the Framework.

Under its current Rules, AFCA will be able to have regard to these standards when resolving individual complaints.

Possible bank-specific obligations

Proposed bank-specific obligations are set out on page 20 of the consultation paper. The preceding text states that *The obligations under this Code are intended to address scams as defined earlier in the paper and do not seek to address unauthorised transactions.*

AFCA believes it is necessary to holistically review the operation of the current provisions for allocating liability for unauthorised transactions under the ePC and the broader treatment of authorised transactions. It can be difficult to determine whether a particular scam or set of circumstances is covered by the ePC and while we understand that there will be a separate process for reviewing that Code, it is essential that there are no gaps or conflicts in terms of what is covered by the ePC and the new Code. It seems preferable that the overarching scams Framework should cover the breadth of scams as they continue to evolve.

Our comments on the possible bank-specific obligations mirror some of our earlier comments about the proposed ecosystem-wide obligations in the CCA. These include that:

- There should be timeframes and specific details about new reforms (including the confirmation of payee reforms and potential introduction of a "freeze switch").
- There should be specific obligations around having efficient and timely means for customers to report scams and get help during a scam.
    - > We have had complaints where customers reported trying to get through to a bank's fraud departments for hours. One customer told AFCA they attended the branch and were told to go home and try again as branch staff would not be able to get through any faster.

> Consumers should be able to report scams 24/7 so that ADIs can act promptly, including by holding or stopping payments.

- There should be more detail about appropriate responses to high-risk transactions e.g., when should they be blocked (for example when the ADI has received notification of a mule account) as opposed to subject to a consumer warning. It is not clear that the current proposals will drive consistent bank responses and processes (noting that it is intended that a firm's anti-scams strategy will not be made public) nor assist AFCA in resolving disputes.
- There should be specific and clear obligations on the role of the receiving banks, including about how recall systems should work in practice
- There should be obligations to record and report on scams complaints dealt with at IDR.

In finalising these obligations, we urge Government to consider how they will in practice drive consistent, higher standards by ADIs. We acknowledge that there have been important initiatives by individual banks (for example NAB announced in July 2023 that it will remove links in text messages to protect its customers, and two other banks followed with similar announcements). However there needs to be system wide, consistent action across the ADI cohort to support disruption and effective consumer education/action. It is not clear how the current proposed Framework would achieve this.

Five priority initiatives that would disrupt or prevent scams: an AFCA perspective

Our complaints experience, and information-sharing with overseas ombudsman schemes that are also dealing with the challenges posed by scams complaints, indicates that the following five areas of reform would greatly assist in the disruption and prevention of scams. We note that (some) Australian banks have committed to some of these initiatives, and some of them are also reflected in the proposed Code obligations in the consultation paper, but more needs to be done to ensure that they are done consistently and in a timely way. We present these for consideration in further development of the mandatory Codes.

1. Confirmation of Payee

- Currently Australian payments through the BECS system only match BSB and account number. This has facilitated scam payments where the account name provided by the scammer differs from the real account name. This occurs in email compromise scams and in some investment and buying and selling scams.
- Under the Bank Accord announced by the ABA on 24 November 2023, a new confirmation of payee system will be rolled out across all Australian banks. The ABA said that design of the new system will start straight away and it will be built and rolled out over 2024 and 2025.

- Based on our information, confirmation of payee could assist in disrupting up to 15% of all scams – it is the major weapon against invoice hacking scams and many impersonation scams and is an important protection for small business victims.
- AFCA strongly supports this measure and seeks confirmation that this will be implemented in a timely and effective way and across the entire ADI cohort.
- In the UK, confirmation of account name BSB and account number is now mandatory for the major banks (since 2020) and in October 2022 it was announced it will expand to 400 other banks and financial firms. The first tranche was due to be compliant by October 2023 and the remainder by October 2024. Confirmation of payee is also available across much of Europe.

2. More secure delivery of Codes (OTPs) and communication – removing links.

- One-time passwords (OTP) are security Codes generally sent by SMS when a consumer is paying someone new, adding a device to a wallet or making another change to their online banking.
- Many scams involve the scammer asking the person to provide these Codes sent by the financial firm. Often the scammer can convince the person the Codes to perform a transaction are for a purpose other than to perform a transaction. Where the scammer has remote access of a mobile device the OTPs can be received by the scammer and deleted without the person knowing they have received them.
- It would assist if OTPs were used consistently across all ADIs. Some banks say they will never ask for an OTP, while others require it as part of their verification processes. Communication could be standardised to avoid confusion about their purpose. An even stronger response would require Codes to be delivered in banking apps, or a new method of authentication could be devised which takes into account how scammers have been abusing OTPs.
- In Malaysia they migrated from SMS OTPs to a more secure in-app authentication method from 22 June 2023.
- ADIs could move away from all links and Codes delivered by SMS. As noted earlier, while some banks have announced that they will be doing this, it is not happening consistently across all ADIs or in a specific timeframe to support consumer awareness. This measure was mandated in Singapore from January 2022 for retail customers.

3. Customer Empowerment and further authentication

- Consumers should be more empowered to effectively control access to banking products and to set appropriate limits to minimise the risk of losses.
- Various limits for different payment services such as pay anyone, BPay etc should be more transparent and customer driven. Customers should be informed of default limits and be able to lower limits on various payment methods easily. There should be lower default limits particularly for debit cards. Limit increases should require additional authentication.

- Customers should be able to freeze or lock their own accounts if they are worried about third parties accessing the account or feel they have made a payment to a scammer. This could also be done if customers know they will not be requiring access to a particular account for a period while, for example, they are away or due to illness.
- In Singapore from June 2022, banks have introduced an in-banking app emergency self-service “kill switch” for customers to suspend their bank accounts quickly if they suspect these have been compromised. We note the bank specific obligations in the consultation paper include mention of a “freeze switch” but this has no detail yet about timing or application.
- Further authentication should be required if a customer seeks to set up internet banking or access internet banking on a new device, add a digital card to a wallet on a new device or change their internet banking passC\code.
- Malaysia has had verification and a cooling-off period for first-time enrolment of e-banking services since June 2023.
- Singapore has had a cooling-off period before implementation of requests for key account changes such as customer contact details since January 2022. There is also notification to the existing mobile number or email registered with the bank when there is a request to change a customer’s mobile number or email.
- Since January 2022 Singapore has had a delay of at least 12 hours before activation of new soft token on a mobile device and in Malaysia from June 2023 a digital card can only be added to a single mobile device. These initiatives would assist with the digital wallet scams AFCA is currently seeing.

4. Consistent Restrictions on Crypto

- According to Scamwatch, Australians lost $221 million to cryptocurrency scams last year24. Funds can be channelled through a legitimate crypto platform, or the scammer convinces the person to provide details of their crypto account/wallet and takes the funds from the account/wallet.
- Restrictions, delays and/or frictions should be considered for crypto transfers. In the UK, banks introduced friction into payments to crypto platforms because of the reversal of the onus of proof under the contingent reimbursement Code. TSB in the UK, which offers a fraud refund guarantee, does not allow payments to crypto platforms.
- Given the large number of scams involving crypto, we think it would make sense to introduce measures such as a 24-hour hold on first payments to a crypto platform, or a dollar limit per payment or period, which could be changed if the customer contacts the branch.
- Consideration should also be given to banning the use of credit cards to purchase crypto, similar to the restrictions on the use of credit cards for gambling.

[24] Minister for Financial Services - Reference to Scamwatch Report on Crypto losses

- Different Banks have introduced different measures in response to retail crypto risk. For example:
  - From May 2023 Westpac blocked payments to Binance and other crypto platforms it has designated high risk.
  - From 8 June 2023 CBA made changes to decline or hold on certain payments to crypto exchanges, and blocked exchanges with high scam activity.
  - CBA has changed its terms and conditions so no more than $10,000 can be sent to a crypto exchange in a month.
  - NAB announced on 7 July 2023 that it will no longer send funds to particular crypto platforms. Also, it will be implementing a 24-hour hold for first time payments and monthly limits on payments to crypto platforms.
  - ANZ has indicated it will also be blocking certain high-risk payments to crypto platforms. It may hold first time payments for 72 hours.
- Singapore has banned payments to crypto platforms for retail customers.

5. Recall and liability of the receiving bank

- The ePC sets out a regime for banks to recall funds for mistaken internet payments. Mistaken internet payments are where a person makes a typo in the BSB or account number or selects the wrong account from a drop-down box. The Code prescribes time frames in which requests must be made and when repayments can be made. It also places obligations on the receiving bank around recall.
- Credit card scheme rules also have charge back Codes that can be used to reverse payments.
- For pay anyone and other types of payments there are currently no recall obligations or rules about when funds can be taken from the recipient's account.
- The receiving bank does not have any obligation to respond in a particular time frame or manner for pay anyone scams. The receiving bank often refuses to provide information to the sending bank because of privacy or confidentiality.
- In the UK, legislation provides that the liability for a scam will be shared 50% by the sending and receiving bank in certain circumstances.
- Scams using mule accounts would likely not occur without the ability to open and obtain mule accounts, or at least be reduced if recall functions and liability obligations were introduced.
- When opening accounts, the bank should check the person providing the identification is the genuine owner of the identification – there should be no exceptions for online account opening.
- There should be a greater enforcement focus on people allowing accounts to be used as mule accounts for a fee and people involved in the purchase and sale of bank accounts that can then be used as mule accounts.
- Live data sharing particularly around mule accounts will be invaluable.