Scams—mandatory industry codes

Submission by the Australian Securities and Investments Commission

February 2024

Contents

Executive summary

1 The Australian Securities and Investments Commission (ASIC) makes this submission in response to the consultation paper *Scams—Mandatory Industry Codes* (consultation paper).

2 ASIC supports the introduction of a whole of ecosystem framework that requires banks, telecommunication providers, digital platforms and other businesses to prevent, detect and respond to scams.

3 We consider that there are opportunities to improve the proposed Scams Code Framework in some areas, in particular in relation to:

(a) regulator responsibility for enforcement of the principles-based framework obligations as applicable to the banking sector;

(b) the proposed definition of 'scam';

(c) the content and coverage of the principles-based and sector-specific framework obligations; and

(d) pathways for consumer compensation.

4 Table 1 summarises our responses in this submission to specific questions raised in the consultation paper. Given ASIC's regulatory remit, this submission focuses on the issues as applicable to the banking sector.

Table 1: Overview of ASIC's submission

Topic/submission reference	Summary of ASIC's feedback
Scams Code Framework and multi-regulator oversight (responses to questions 1–4, 7, 43 and 44 of the consultation paper): Section B	The proposed ecosystem-wide principles-based obligations are detailed, and broader in scope than the proposed banking sector code obligations. They are therefore likely to present broader coverage, and a stronger legal basis, for enforcement. Given ASIC's current remit and enforcement role in respect of the banking sector, we consider that ASIC should be empowered to enforce the principles-based obligations in respect of the banking sector, alongside the ACCC. This will enable ASIC to maintain its conduct regulation role for the banking sector, and also mitigate potential inefficiencies for both banks and regulators that would likely arise under the proposed multi-regulator enforcement of the framework. We also propose the introduction of a statutory mechanism for streamlined information-sharing between relevant regulators, to support the efficient exchange of scams-related information and a consistent approach to administration of the framework.

Topic/submission reference	Summary of ASIC's feedback
Definition of 'scam' (responses to questions 8–11 of the consultation paper): Section C	The proposed definition of 'scam' may create workability and enforceability challenges for regulators, businesses, external dispute resolution operators, and consumers. We have not suggested an alternative formulation, but consider that the definition should have the following features: • no 'dishonesty' element, or other subjective element that requires determining the state of mind of the scammer; • use of inclusive language to define the categories of scam activity captured, and a statutory mechanism to update the definition over time; • any carve-outs from the definition (for example, 'unauthorised' conduct) be clearly defined, to avoid unintended limitations on the application of the framework; and • no elements that are difficult to establish, or unable to be established, as at the time of the suspected scam conduct being detected.
Principles-based obligations (responses to questions 15, 16, 23 and 25 of the consultation paper): Section D	ASIC supports the introduction of enforceable, ecosystem-wide, principles-based obligations. We suggest the adoption of additional obligations for: • ongoing monitoring and revision of anti-scam strategies by regulated businesses; • senior management oversight of scams work within regulated businesses; • adequate resourcing of scams function and strategy; and • standardised public reporting requirements as to regulated businesses' anti-scam commitments to customers, and the outcomes of their anti-scam work. We also suggest some revisions to the content of the current proposed obligations, to incorporate evaluative or outcome-based components including for timely action, to bolster scam response and documentation requirements, as well as to extend coverage of the obligations to some specific contexts. We do not support mandating regulator review of anti-scam strategies, and consider regulatory guidance and other publications would better support industry compliance.
Sector-specific codes and standards (responses to questions 35, 37 and 39 of the consultation paper): Section E	ASIC supports the introduction of enforceable banking sector-specific obligations. We recognise that the proposed obligations are preliminary and high level in nature at this early stage. The final obligations will need to be more detailed and specific, to support enforceability by ASIC as well as effective dispute resolution by AFCA. By way of early feedback, we suggest the adoption of additional obligations for receiving banks, standardised public reporting, and to codify effective existing anti-scams initiatives. We also suggest some revisions to the content of the current proposed obligations, to require timeliness of action and incorporate evaluative or outcome-based components, as well as to extend coverage of the obligations to some specific contexts.

Topic/submission reference	Summary of ASIC's feedback
Non-compliance with framework obligations – consumer compensation and penalties (response to questions 33 and 45 of the consultation paper): Section F	Our view is that where a business does not meet its obligations under the framework: • there should be clear and effective pathways for consumer compensation, and compensation should extend to all impacted consumers and not just those who make a report or complaint; and • significant penalties should be able to be ordered by a court where appropriate to incentivise compliance and achieve deterrence, with penalties to be consistent across the scams ecosystem. We also suggest consideration be given to requiring businesses to publish their scams remediation policy and compensation data.

A ASIC's work to combat scams

5 As noted at paragraph 1 of the consultation paper, scams are increasing in volume and sophistication, causing significant financial and other harm to Australian consumers.

6 Combatting scams is one of ASIC's core strategic projects. Our work includes:

(a) disrupting online investment scams by removing or limiting access to investment scam and phishing websites via a website takedown service;

(b) working with other government agencies and industry to coordinate scams disruption strategies, including through the National Anti-Scam Centre (NASC). ASIC and the Australian Competition and Consumer Commission (ACCC) co-lead the first NASC fusion cell, which is focused on combatting investment scams;

(c) influencing our regulated population to strengthen their ability to prevent, detect and respond to scam activity. In 2023, we published Report 761 *Scam prevention, detection and response by the four major banks* (REP 761), an analysis of our review of the scams-related activities of Australia's major banks;

(d) developing communications to support consumers, including publishing consumer education and awareness resources on ASIC's Moneysmart website;

(e) launching a new investor alert list. Consumers can use this list to help inform themselves as to whether an entity they are considering investing in could be fraudulent, a scam or unlicensed; and

(f) taking targeted enforcement action where appropriate to deter scams and to hold scammers to account.

7 Our work combatting scams is one part of the government's Fighting Scams initiative to disrupt scams and protect Australians from financial harm.

8 As combatting scams is also a critical task for industry, we address in the remainder of this submission some opportunities to improve the efficacy of the Scams Code Framework in requiring businesses to prevent, detect and respond to scams.

B Scams Code Framework and multi-regulator oversight

Key points

This section outlines our feedback on questions 1–4, 7, 43 and 44 of the consultation paper.

The proposed ecosystem-wide principles-based obligations are detailed, and broader in scope than the proposed banking sector code obligations. They are therefore likely to present broader coverage, and a stronger legal basis, for enforcement.

Given ASIC's current remit and enforcement role in respect of the banking sector, we consider that ASIC should be empowered to enforce the principles-based obligations in respect of the banking sector, alongside the ACCC.

This will enable ASIC to maintain its conduct regulation of the banking sector, and also mitigate inefficiencies for both banks and regulators that would likely arise under the proposed multi-regulator enforcement of the framework.

We also propose the introduction of a statutory mechanism for streamlined information-sharing between relevant regulators, to support the efficient exchange of scams-related information and a consistent approach to the administration of the framework.

Questions 1–4, 7, 43—Structure of the Scams Code Framework and multi-regulator oversight

9 The consultation paper proposes the following model for the framework and its administration:

(a) principles-based obligations applicable to all entities across the scams ecosystem to be inserted into primary legislation—for example the *Competition and Consumer Act 2010*—and administered by the ACCC alone; and

(b) additional sector-specific obligations to be set by codes and standards, with ASIC to monitor and enforce the scams code for the banking sector as established under ASIC-administered legislation.

10 We support the overall structure of the framework, with the overarching principles-based obligations facilitating broad consistency in anti-scam standards across sectors, supplemented by more tailored sector-specific code requirements.

11 However, for the banking sector, we consider that an alternative setting for enforcement of the principles-based obligations is likely to be more effective.

Role of regulator for principles-based obligations

12 As currently proposed, the principles-based obligations are detailed. They appear substantially broader in scope than, and to subsume the coverage of, the proposed code obligations for the banking sector. The principles-based obligations are therefore likely to present broader coverage, and a stronger legal basis, for enforcement.

13 Consistent with this, the consultation paper suggests that the ACCC would have a strong role in monitoring and taking enforcement action for systemic or significant breaches of framework obligations across the ecosystem, including for the financial sector.

14 Given ASIC's current remit and enforcement role in respect of the banking sector, we do not consider that enforcement action in respect of systemic or significant breaches of framework obligations in that sector should be exclusively reserved for the ACCC. There are a range of circumstances where it may be more efficient and effective for ASIC to take such action. Therefore, for the reasons that follow, we consider that ASIC should be empowered to enforce the principles-based obligations in respect of the banking sector, alongside the ACCC.

ASIC enforcement of principles-based obligations for the banking sector

15 As Australia's integrated corporate, financial services, consumer credit and markets regulator, ASIC has a broad existing regulatory remit in respect of the banking sector. We play a significant role in conduct regulation for the sector, and regularly pursue enforcement action against banks where serious non-compliance is identified.

16 Under our current remit, there are a range of existing statutory obligations enforceable by ASIC that apply to banks and that could be relevant in the scams context, including:

(a) obligations applicable to holders of Australian Financial Services Licences and Australian Credit Licences under s912A of the *Corporations Act 2001* (Corporations Act) and s47 of the *National Consumer Credit Protection Act 2009* respectively, including the 'efficiently, honestly and fairly' obligations, and requirements for internal dispute resolution (IDR) and external dispute resolution (EDR) arrangements;

(b) obligations under the Financial Accountability Regime that commence for authorised deposit-taking institutions on 15 March 2024, including to conduct business with due skill, care and diligence;

(c) consumer protection provisions applicable to the supply of financial services under the *Australian Securities and Investments Commission Act 2001* (ASIC Act) and Corporations Act, including prohibitions on unconscionable conduct and false, misleading or deceptive conduct;

(d) criminal offence provisions under the *Criminal Code Act 1995* (Criminal Code) and State-based criminal legislation, including prohibitions on fraudulent and deceptive conduct; and

(e) requirements to report potential statutory breaches to ASIC as well as the Australian Prudential Regulation Authority (APRA), and to provide particular information when required by ASIC.

17 Areas of overlap are likely to arise between the above existing obligations administered by ASIC, the principles-based obligations, and the banking code obligations. However, under the division of regulator responsibility proposed by the consultation paper, the ACCC alone would have the responsibility to enforce the principles-based obligations. This setting will likely give rise to the following issues:

(a) **For banks**: This may result in added compliance burden and complexity for the banking sector, given the potential need for banks to engage with two different regulators (or three if APRA is also engaged) in respect of the same or related conduct.

(b) **For regulators**: This may create regulatory complexity for ASIC and the ACCC. While ASIC and the ACCC closely engage on anti-scam work, enforcement of overlapping obligations is nevertheless likely to result in some duplication of regulatory effort.

18 In our view, the above issues cannot be fully addressed through regulator engagement and coordination, or through the use of delegations of power, unless current delegation mechanisms are reformed.

19 As an alternative to the division of regulator responsibility for enforcement as set out in the consultation paper, we propose that ASIC be empowered to enforce the principles-based obligations for the banking sector, alongside the ACCC. This could be achieved by mirroring the principles-based obligations in ASIC-administered legislation.

20 This approach would enable ASIC, where appropriate and in consultation with the ACCC, to enforce all banking sector scams-related conduct, and thereby:

(a) maintain our conduct regulation role in respect of the banking sector, fully utilising our existing financial services regulation experience and expertise;

(b) mitigate the inefficiencies addressed in paragraph 17 above, as ASIC and the ACCC can coordinate responsibilities regarding enforcement of the principles-based obligations for the banking sector, and put in place arrangements to streamline regulatory engagement by the sector, reducing inefficiency and complexity; and

(c) support the efficient administration of obligations for future sectors brought within the framework where ASIC has existing or forthcoming oversight responsibilities, such as the superannuation sector.

21 ASIC and the ACCC are familiar with navigating shared responsibilities, in light of our respective administration of the consumer protection provisions in the ASIC Act which replicate those contained in the Australian Consumer Law. Our agencies have well-established and effective arrangements in place to coordinate activity and share information on issues of joint interest, including as to our present anti-scams work. We consider that similar arrangements could be readily established to ensure the efficient administration of the principles-based obligations in respect of the banking sector.

Question 44—information sharing between regulators

22 ASIC agrees with the observation in the consultation paper that regulators need to work closely together to ensure a consistent and whole-of-ecosystem approach is taken to administration and enforcement of the framework.

23 To support this objective, we propose that consideration be given to the introduction of a statutory mechanism for streamlined information-sharing, to enable the efficient exchange of potentially large volumes of scams information between ASIC, the ACCC, and the Australian Communications and Media Authority (and potentially also other agencies and bodies such as AUSTRAC, the Australian Taxation Office, and the Australian Federal Police). Process requirements attaching to current information sharing mechanisms can slow the timely release of information.

C Definition of ‘scam’

Key points

This section outlines our feedback on questions 8–11 of the consultation paper.

Some aspects of the proposed definition of ‘scam’ may create challenges for compliance and enforceability, give rise to uncertainty as to coverage of scam conduct under the framework, and detract from the effectiveness of framework obligations.

While we have not suggested an alternative formulation of the definition of ‘scam’, we propose that the definition incorporate particular features in order to address these issues.

Definition of ‘scam’

24 The definition of ‘scam’ proposed by the consultation paper is as follows:

> A scam is a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means.

25 ASIC’s understanding is that the definition of ‘scam’ will essentially operate as a threshold requirement for the application of the framework. That is, for any of the framework obligations to apply, the definition of scam needs to first be satisfied.

26 It is therefore important that the definition of ‘scam’ not only achieves the intended coverage of scam conduct, but is also workable for industry compliance as well as regulatory enforcement purposes, and supports the effectiveness of the framework obligations more generally. Our view is that aspects of the proposed definition detract from these objectives.

27 To address the issues considered further below, while we have not suggested an alternative formulation of the definition of ‘scam’, we consider that any definition adopted should have the following features:

(a) no ‘dishonesty’ element or other subjective element that requires determining the state of mind of the scammer;

(b) use of inclusive language to define the categories of scam activity captured, and a statutory mechanism to update the definition over time;

(c) any carve-outs from the definition (for example, ‘unauthorised’ conduct) be clearly defined, to avoid unintended limitations on the application of the framework; and

(d) no elements that are difficult to establish, or unable to be established, as at the time of the suspected scam conduct being detected.

Questions 8 and 11—impact of subjective requirements

28 The proposed definition of 'scam' contains a number of subjective elements that may be difficult or impossible to establish, particularly as at the time of the suspected scam conduct being detected: 'dishonest', 'designed to obtain' and 'by deceptive means'.

29 Firstly, the proposed definition requires scam conduct to be 'dishonest', which aligns with definitions of fraudulent conduct under the Criminal Code.

30 Definitions of 'dishonest' vary across existing Commonwealth legislation, with different definitions applying under the Criminal Code and Corporations Act. However, each of these definitions require, at a minimum, determination of the defendant's subjective state of mind—their beliefs, knowledge, or intent regarding their conduct.

31 In the context of the framework, establishing the state of mind of a scammer in order to prove dishonesty will likely be challenging for regulators, regulated businesses and consumers alike. This could have serious unintended consequences for the application of the framework. For example:

(a) **For regulators**: obtaining evidence of a scammer's actual state of mind to establish dishonesty will likely be difficult, as the scammer responsible may not be identifiable, and most scammers are also unlikely to comply with or be subject to Australian regulatory investigation processes. This could mean that the definition of 'scam' is unable to be satisfied in most cases, with framework obligations unenforceable.

(b) **For EDR operators, businesses, and consumers**: information about a scammer's actual state of mind sufficient to demonstrate dishonesty is unlikely to be available to EDR operators, regulated businesses or consumers. This may create considerable uncertainty for these parties as to whether the framework obligations apply.

32 Similar issues arise with the 'designed to obtain' and 'by deceptive means' elements of the proposed definition, which are also directed to the state of mind of the scammer, and thus challenging to establish:

(a) '**Designed to obtain**': The proposed definition requires the scam to be 'designed to obtain personal information or a financial benefit'. The scammer's objective in perpetuating a scam may not be apparent or readily ascertainable as at the time of the suspected scam conduct being detected.

(b) '**By deceptive means**': Whether the scam conduct is deceptive turns on the scammer's intention, and will in many cases be unable to be conclusively determined as at the time of the suspected scam conduct being detected; for example, a scam involving promises by the scammer to do a future act.

33 In light of the above concerns, we suggest that the 'dishonest' requirement be removed from the definition of 'scam', and that no element of the definition of 'scam', however drafted, should be subjective in nature and require regulators, businesses or consumers to determine the state of mind of the scammer.

34 Consideration could be given to instead examining the apparent or likely nature and purpose of the conduct, or applying presumptions as to the nature and purpose of the conduct, to enliven the framework obligations.

Question 9—'invitation, request, notification, or offer'

35 The consultation paper states that the framework is intended to cover a broad range of scam categories including investment, romance, phishing, employment, and remote access scams. The methodology employed by these types of scams is proposed to be captured by the phrase 'invitation, request, notification or offer' in the definition of 'scam'.

36 Our view is that this terminology may not be sufficiently broad to capture all intended types of scam activity. For example, romance scam conduct may not be fully captured by these categories, given the interpersonal and variable nature of the interactions between scammer and scam victim.

37 Further, embedding a prescriptive list of scam activities into the definition of 'scam' may risk the definition becoming outdated over time, in light of evolving scams behaviour as well as technological advances.

38 We suggest that less prescriptive terminology be used to define the categories of scam activity. The addition of a statutory mechanism for future updating or expansion of the definition of 'scam' would also assist, to ensure sufficient flexibility to capture new and emerging categories of scams over time.

Question 10—scope of harms

39 The consultation paper states that the definition of 'scam' is intended to exclude 'unauthorised fraud', being conduct that does not involve deception of a consumer into 'authorising' the fraud. In the banking sector context specifically, it further notes that:

(a) the obligations under the banking-sector specific code are not intended to address unauthorised transactions; and

(b) obligations of banks in relation to unauthorised transactions will be considered as part of the future review of the ePayments Code.

40 It is unclear whether the terms ‘unauthorised fraud’ and ‘unauthorised transactions’ are intended as synonymous, when used in the consultation paper in relation to the banking sector. While the concepts of ‘authorised’ and ‘unauthorised’ transactions may be familiar and relevant to the banking sector, the applicability and relevance of this distinction to telecommunications providers and digital platforms is less clear.

41 In the banking sector context, distinguishing between authorised and unauthorised transactions is not always straightforward. For example, the consultation paper indicates that both remote access and phishing scams are intended to be covered by the framework. However, depending on the particular circumstances and methodology of the scammer, these scams may involve scammers stealing information from victims that is then used by the scammer to make ‘unauthorised’ transactions on the scam victim’s bank account.

42 ASIC’s view is that any carve-outs from the definition of ‘scam’ will need to be clearly described, to promote certainty and avoid impracticable or unintended limitations on the application of the framework.

43 In the banking context specifically, we suggest further consideration be given to the terminology used, including to ensure adequate coverage of authorised and unauthorised transactions across the framework and ePayments Code as well as a clear demarcation of the circumstances in which each apply.

D Ecosystem-wide principles-based obligations

Key points

This section outlines our feedback on questions 15, 16, 23 and 25.

ASIC supports the introduction of enforceable, ecosystem-wide, principle-based obligations. Based on our findings in REP 761 as well as practices in peer jurisdictions, we suggest the adoption of additional obligations, and some revisions to the content and coverage of the current proposed obligations, to ensure these obligations are effective to address scams.

We do not support mandating regulator review of anti-scam strategies, and consider regulatory guidance and other publications would better support industry compliance.

Ecosystem-wide principles-based obligations

44 ASIC supports the introduction of enforceable, ecosystem-wide, principle-based obligations into primary law.

45 We agree that these overarching obligations should be flexible and scalable in order to apply across sectors, and be capable of responding to the evolution of scam methodologies and typologies.

46 We also agree with the approach adopted of requiring proactive action on the part of businesses to prevent, detect, disrupt and respond to scams. A problem of this scale and complexity requires a whole-of-ecosystem response.

47 Drawing on our anti-scam work and the regulatory approach taken in peer jurisdictions, we consider that the following additional principles-based obligations should be considered, as part of ensuring the framework achieves effective and robust coverage:

(a) ongoing monitoring and revision of anti-scam strategies by regulated businesses;

(b) senior management oversight of scam prevention, detection and reporting within regulated businesses;

(c) adequate resourcing of scams function and strategy; and

(d) public reporting requirements as to regulated businesses' anti-scam commitments to customers, and the outcomes of their anti-scam work.

48 Further, while we support the intent of the proposed principles-based obligations, we consider that there are gaps and a lack of specificity in the

content and coverage of these obligations as currently framed, which may undermine their intended effect. We suggest amending these obligations to:

(a) incorporate evaluative or outcome-based components, including for timely action;

(b) bolster scam response and documentation requirements; and

(c) extend coverage of the obligations to some specific contexts.

Questions 15 and 23—additional obligations and anti-scam strategy

Monitoring and revising anti-scam strategies

49 We suggest the introduction of an obligation for regulated businesses to proactively monitor the outcomes of their anti-scam strategy, and to revise the strategy if objectives are not being met.

50 Such an obligation would ensure that businesses maintain scams strategies that are up to date and fit for purpose, and reduce the risk of businesses relying on outdated or ineffective strategies for extended periods of time. ASIC's REP 761 found that of Australia's four major banks:

(a) only one had carried out a review of their scams prevention, detection and response capabilities over the preceding three years (as at the time of ASIC's review);

(b) there was limited, or—in some cases—no monitoring by the banks of the effectiveness of their scam awareness and education initiatives; and

(c) the overall approach to scams strategy was variable and overall less mature than expected.

51 Given the evolving nature of scams, anti-scam strategies that may have once been appropriate will become outdated and less effective as scammers find new vulnerabilities to target, new ways to deceive consumers, and new methods to avoid detection. The availability of new technologies to improve systems, products or service delivery, or the adoption of process changes, may also necessitate an update of a business's anti-scams strategy and capabilities. More generally, even a well-designed anti-scam strategy may have unforeseen issues or inadequacies.

52 We therefore consider proactive monitoring and revision of an anti-scam strategy as critical to ensure that anti-scam activities remain fit for purpose and drive continuous improvement.

53 Question 23 of the consultation paper asks how often businesses should be required to review their anti-scam strategies and whether this should be legislated. In addition to any obligation imposed to review the strategy at set

intervals, we suggest that there be an overarching obligation to regularly and proactively monitor performance, and revise the strategy if circumstances exist suggesting that the strategy is no longer suitable. This approach allows for flexibility and reduces the risks of a 'one-size-fits-all' review period, which may not keep up with a fast-evolving scams landscape.

Senior management oversight of scams work

54 We also suggest consideration be given to introducing a requirement for regular reporting within regulated businesses to senior management and board level on a business's anti-scam work, as well as on the scams landscape. This reporting could capture the scams threat environment, operational efficiency and effectiveness of scams initiatives, as well as customer experience and outcomes.

55 REP 761 found that only two of the major banks provided detailed and regular internal reporting to their boards about scams that had a focus on customer experience and outcomes. Regular reporting will ensure continued internal focus on anti-scam activities at senior management and board levels within regulated businesses.

Resourcing

56 In our view, the principles-based obligations should also include a requirement for businesses to adequately resource their scams functions and strategy. This requirement should be flexible and scalable to account for various types and sizes of businesses.

57 In line with the findings of REP 761, businesses should have sufficient resources for the timely and effective implementation of their anti-scam strategy, including proportionately appropriate staffing numbers to deal with complaints or scam reports in a timely, fair and effective manner. This would also include resourcing to deal with intermittent spikes in scam volumes.

58 Such obligations would also be consistent with existing requirements applicable to banks with respect to resourcing of their IDR function, as set out in ASIC Regulatory Guide 271 *Internal dispute resolution* (RG 271).

Transparency

59 We suggest consideration be given to further transparency requirements that would not require disclosure of sensitive information useful to scammers. This could include the publication of anti-scam commitments to consumers, and ongoing public reporting as to work delivered against these commitments.

60 Such public reporting should ideally be subject to regulatory requirements, to ensure reporting is standardised and uses consistent data definitions, enabling comparison of business performance.

61 The current proposed obligations require transparent complaints handling processes and the provision of particular information to consumers, but do not otherwise mandate transparency mechanisms.

62 Additional transparency mechanisms have been adopted in other jurisdictions. For example, the UK Online Fraud Charter agreed between the UK government and the technology sector requires firms to provide transparency reports on how platforms are working to keep users safe.

63 There are benchmarking and accountability benefits to mandating public reporting in some areas, and ASIC agrees with the consultation paper that publication of anti-scam measures would help build industry and consumer confidence in businesses and the framework. We also agree that obligations should not be imposed that would require publication of operational or technical information that may be useful to scammers.

Question 16—content and coverage of proposed obligations

Suggested improvements to the content of obligations

Adequacy of required action

64 A number of the obligations only require businesses to put particular arrangements in place (such as an anti-scam strategy or anti-scam systems), or to 'seek to' take particular action (such as to detect, block, verify and trace scams).

65 In ASIC's experience, requirements to merely have processes or methods in place, or to 'seek to' take action are not sufficient to ensure that appropriate arrangements are implemented, that adequate action is taken, or that the desired outcomes are achieved. These settings could also lead to inconsistency in industry practice.

66 To ensure meaningful implementation of the framework obligations, we consider that each relevant principles-based and banking code obligation should be revised to incorporate evaluative, quality or outcome-based components, such as requiring processes and strategies to be effective, for all reasonable steps to be taken where action is required, and for any action to be taken in a timely way.

67 Timely action to prevent, detect, and respond to scams is critical to minimising consumer harm. While some of the proposed obligations contain

a timeliness requirement, it is missing from others, such as in the proposed obligations for businesses to seek to detect, block, prevent, verify, trace, and share data on scams.

68 In our view, all relevant principles-based and banking code obligations should also incorporate a timeliness requirement. We note that the UK Online Fraud Charter contains a number of signatory commitments that integrate timeliness, including commitments to 'take action against fraudulent content and users **straight away**', 'remove fraudulent content **immediately'**, and 'action user reports **as swiftly as possible'**.

Responding to scams reports by consumers

69 The consultation paper proposes that businesses be required to take all reasonable steps to prevent further consumer loss and treat consumers fairly and consistently, once a consumer has identified they have been affected by a scam.

70 We support this obligation and suggest that it extend to requiring:

(a) consumers to be treated fairly and consistently regardless of the method or channel of contact (i.e. 'no wrong door');

Note: REP 761 observed that scam victims who made a complaint to the four major banks were more likely to receive some form of compensation than those who did not. REP 761 found that a contributing factor to low reimbursement by some of the four major banks was scams response teams having less scope or authority compared with complaints teams.

(b) businesses to offer flexibility in the methods or channels in which a customer may contact them to report a scam or make a complaint. This would be consistent with existing IDR requirements applicable to banks for lodgement of complaints, as set out in RG 271 at RG 271.136; and

(c) businesses to ensure staff tasked with responding to scam victims have appropriate authority to fairly and efficiently respond to reports of scams.

71 We also suggest that this obligation become enlivened once a business becomes aware of a scam and that consumers have been impacted. That is, treatment of consumers should not depend on whether the consumer has reported the scam. The ACCC's 2021 *Targeting scams report* found that around a third of scam victims do not report the scam to anyone. There are serious financial, social and emotional impacts of scams, including the experience of shame and stigma, which can operate as barriers to reporting.

Documenting approach to customers experiencing vulnerability

72 In our view, the proposed obligation on businesses to keep records of incidences of scams and actions taken in response should extend to cover the

end-to-end scam journey, including requiring documentation of the approach to vulnerable consumers.

73 In the banking context, REP 761 observed that banks should identify and document their approach to customers experiencing vulnerability, to ensure that extra care is taken when responding to such customers affected by scam activity.

Suggested improvements to coverage of obligations

Misuse of services

74 We support the proposed obligation on businesses to take all reasonable steps to prevent misuse of its services, and suggest that:

(a) this proposed obligation extend to misuse of business brands and brand assets. This would capture, for example, scams involving bank impersonation and use of business logos, colour schemes, or jingles. REP 761 found that the four major banks were active in monitoring for, and responding to, the fraudulent misuse of their brand and brand assets.

(b) the proposed obligations for scam disruption and response apply to identified misuse of services, business brands and brand assets.

New technologies

75 We support the proposed obligation for businesses to implement anti-scam systems that are responsive to new technologies.

76 This obligation is consistent with industry initiatives such as the Australian banks' Scam-Safe Accord, committed to by members of the Australian Banking Association (ABA) and the Customer Owned Banking Association (COBA) to combat scams and deliver greater protections. The accord commits all banks to adopting further technology and controls to help prevent identity fraud, including major banks using at least one biometric check for customers opening accounts online by the end of 2024.

77 We suggest that 'new technologies' be broadly defined to capture those used to build and enhance banking applications (apps) and websites, in light of online banking now being the sole means of accessing banking services for many consumers, particularly given the extent of bank branch closures across Australia.

Clarification of concepts

78 Some aspects of the proposed obligations are expressed in vague or unclear terms, which may present implementation challenges for industry, regulators and EDR operators. For example, for some of the regulated sectors, it is

unclear what it means for consumers or users to have 'tools to verify information in real time'; what is required from businesses to 'verify and trace' scams; and the nature and extent of the 'anti-scam systems' required to be implemented by businesses.

79 We suggest that consideration be given to the use of definitions or examples that enhance clarity and workability.

Question 25—regulator review of anti-scam strategy

80 What constitutes an appropriate anti-scam strategy will be different for each regulated business, depending on their size, business model, services offered, customer base, and other factors.

81 As addressed earlier in this submission, anti-scam strategies will likely also need regular revision over time to remain fit for purpose, given the evolving scams landscape as well as technological advances. The number of regulated businesses, and thus the volume of anti-scam strategies, will also increase materially over time as additional sectors are brought into the framework.

82 In light of the above, mandating regulator review would likely have significant and ongoing resourcing implications for regulators. We consider that industry compliance in this area would be better supported through the development and issue of regulatory guidance, and release of publications such as REP 761 following regulator reviews of businesses' compliance with framework obligations.

E Banking sector code obligations

Key points

This section outlines our feedback on questions 35, 37 and 39.

ASIC supports the introduction of an enforceable scams code for the banking sector, noting that the final version of the code obligations would need to be more detailed and specific in order to be enforceable and to support effective dispute resolution.

We also suggest some additional obligations be adopted, and revisions made to the content and coverage of the current proposed obligations.

Banking sector code obligations

83 ASIC supports the introduction of an enforceable scams code for the banking sector, to be established under ASIC-administered legislation.

84 We recognise that the current proposed banking code obligations are necessarily preliminary and high level in nature at this early stage of the reform process. The final framing of these obligations will need to be more detailed and specific, in order to support:

(a) enforceability by ASIC, thereby driving industry compliance with the requirements; and

(b) effective dispute resolution by the Australian Financial Complaints Authority (AFCA).

85 By way of early feedback, we address below some suggested additional obligations, and some opportunities to improve the content and coverage of the current proposed obligations.

86 More broadly, we agree with the commentary in the consultation paper that obligations for banks should be tailored to their role in the scams ecosystem. While a level of cross-sector consistency is desirable, we consider this can be achieved through the principles-based obligations, and that the sector-specific code obligations should reflect the different functions of each sector and the differing opportunities each sector has to prevent or address scams in the course of the scam lifecycle.

Question 35—additional obligations

Obligations as a receiving bank

87 Banks that receive scam funds are a crucial link in the scams ecosystem, and play an important role in preventing and responding to scams.

88 ASIC's view is that clear, robust and enforceable anti-scams obligations should apply to both sending and receiving banks.

89 While we acknowledge the proposed obligation for receiving banks to revert a transfer within 24 hours of receiving a recall request from a sending bank, consideration should be given to additional tailored obligations for receiving banks. This could include requirements for receiving banks to quickly freeze funds after receiving a recall request; to quickly share information about fund receipts and transfers; and to provide accurate and timely information to their own customers who may have been impacted by a scam.

Transparency

90 We repeat our feedback at paragraphs 59–63 about the need for transparency, and suggest that consideration be given to introducing requirements for standardised public reporting of banks' anti-scam commitments to their customers as well as their anti-scam work.

91 In addition to benchmarking and accountability benefits, such reporting by banks could also provide a valuable indicator of whether the framework is working effectively to reduce scam losses, as the banking sector holds the most data about consumer outcomes at the end of the scam life cycle.

Effective anti-scam practices

92 We agree with the suggestion in the consultation paper that effective voluntary scams practices may be lifted into legislation as ecosystem-wide or sector-specific framework obligations.

93 In the banking context, there is currently variation in banking practices, and codifying good practices would deliver industry-wide consistency, as well as providing consumers with additional certainty about how they should expect to engage with their bank.

94 We encourage consideration to be given to adopting as mandatory requirements for the banking sector measures deployed domestically, including the commitments made as part of the Scam-Safe Accord, as well as industry-wide banking practices adopted in other jurisdictions.

Questions 37 and 39—content and coverage of proposed obligations including timeframes

Suggested improvements to content of obligations

Adequacy of required action

95 The current proposed banking code obligations appear almost wholly process-focused, requiring banks to 'implement processes' or 'have in place methods'. The obligations do not address the required quality of these processes (for example, for the processes to be **adequate**), or of the resulting outcomes (for example, for the processes to be **effective**).

96 This framing increases the risk of low quality and inconsistent anti-scam practices being implemented across the banking sector, to the detriment of consumer outcomes. The availability of consumer redress, and ability for ASIC to require improvements to these practices, will also be severely limited if the obligations only require processes to be in place without regard to their adequacy or effectiveness.

97 We repeat our feedback at paragraphs 64–66 above on the need for framework obligations, including all relevant banking code obligations, to incorporate evaluative, quality or outcome-based components, in order to ensure meaningful implementation.

98 We also repeat our feedback at paragraphs 67–68 above on the need for timeliness requirements, and propose that such a requirement (for example, to act 'quickly', 'immediately' or in a 'timely manner' as appropriate) be incorporated into each banking code obligation that does not currently contain one.

Information sharing

99 Related to the above, the current proposed banking code obligation for information sharing between banks only requires banks to 'have in place methods or processes' to share information with other banks about likely scam accounts and transactions.

100 We suggest that this requirement be enhanced, to ensure that banks undertake effective information sharing with other banks about suspected scams.

101 Efficient and effective intelligence sharing between banks would allow banks access to critical information about scams needed to actively protect their consumers and assist with fund recovery where possible, and facilitate their compliance with other framework obligations.

Suggested improvements to coverage of obligations

Verification of transactions

102 We support the inclusion of an obligation to verify transactions. We suggest that meeting this obligation should not rely solely on verification by the consumer, where other verification mechanisms are available and appropriate, given the ability for scammers to use social engineering or other tactics to coach consumers through many verification processes.

Scam accounts

103 The current obligations require action by banks to address accounts that are 'likely to be or [are] scams'. Though this wording would cover accounts held directly by scammers, it is less clear how it would apply to other arrangements. For example, where the account of a customer is being used by a scammer to receive and transfer scam proceeds, but the customer is the unknowing victim of a money mule scam.

104 We suggest the drafting of the relevant banking code obligations reflect the actions required to respond to all types of scam-related account arrangements.

Consumers experiencing vulnerability

105 We support the proposed obligation for banks to have processes to identify consumers at higher risk of being targeted by a scam.

106 We suggest that these 'vulnerable cohorts' include situational vulnerability, to recognise that any individual may experience scam vulnerability as a result of factors including life events, temporary difficulties, and varying personal or social characteristics.

107 We agree with the proposed obligation for additional steps to be taken for these vulnerable cohorts, and note this may require consideration of situational vulnerability in relation to staff training, prevention, detection and disruption of scams, and responding to scams reports and complaints. Consideration of situational vulnerability might similarly be relevant to other sectors beyond the banking context.

F Non-compliance with obligations—consumer compensation and penalties

Key points

This section outlines our feedback on questions 33 and 45 of the consultation paper.

We consider that where a business does not meet its obligations under the framework:

- there should be clear and effective pathways for consumer compensation, and compensation should extend to all impacted consumers and not just those who make a report or complaint; and
- significant penalties should be able to be ordered by a court where appropriate in order to incentivise compliance and achieve deterrence, with penalties to be consistent across the scams ecosystem.

We also suggest consideration be given to requiring businesses to publish their scams remediation policy and compensation data.

Question 33—consumer compensation

Clear and effective pathways for compensation

108 ASIC supports the proposal in the consultation paper that if a business does not meet its obligations under the framework, internal and external dispute resolution mechanisms should operate where applicable to ensure consumers have access to appropriate redress.

109 We consider that the pathways for consumer redress under the framework need to be clear and effective. REP 761 found that the four major banks adopted inconsistent and generally narrow approaches for reimbursement and compensation, and no bank had a fully documented bank-wide policy for reimbursement or compensation as at the time of ASIC's review. We also observed inconsistencies in the approach taken to reimbursement and compensation across different teams within the same bank (for example, the scams team versus the complaints teams).

110 In our view, clear and effective pathways require:

(a) further specificity in the framing of the ecosystem-wide and sector-specific framework obligations (as addressed in previous sections of this submission);

(b) clarity concerning the required linkage between breach of a framework obligation and consumer compensation entitlements; and

(c) clarity concerning the apportionment of consumer compensation between multiple responsible regulated businesses, for example between businesses in different sectors, or between sending and receiving banks.

Note: Peer jurisdictions have implemented apportionment. In the UK, consumer reimbursement for scams is split equally between sending and receiving firms.

111 The above will support businesses to resolve more complaints and reports at earlier stages, such as through IDR processes, and also assist EDR operators to determine any compensation payable if complaints cannot be resolved through IDR. Pre-EDR resolution of scam issues would ease pressures on EDR operators such as AFCA, which has experienced significant increases in complaints about scams. In the 2022–23 financial year, AFCA saw a 46% rise in serious financial crime and scam-related complaints, and is now receiving an average of more than 500 complaints per month.

Note: See *Scam complaints* on the AFCA website.

112 We note for completeness that where a business is aware that it has not met its obligations under the framework, it should remediate all identifiable impacted consumers, and not just those who make a report or complaint. As addressed at paragraph 71 above, it is common for scams to not be reported.

Reporting of compensation information

113 We suggest consideration be given to mandating publication of scams remediation policies and public reporting as to compensation data, to complement the transparency requirements we proposed earlier in this submission.

114 These reporting measures will improve accountability, enable benchmarking, and facilitate ongoing assessment of the effectiveness of the framework in reducing scam losses.

Question 45—penalties for breaches

115 ASIC's experience is that the availability of significant pecuniary penalties is key to incentivising compliance and achieving deterrence. Having regard to the importance of the framework and the large size of many industry participants in each of the sectors subject to the framework, we consider that significant penalties should be able to be ordered by courts for breaches of both the ecosystem-wide and sector-specific framework obligations.

116 We also support a consistent approach to penalties across the scams ecosystem, as instances of scam conduct often span multiple sectors.

Key terms

Term	Meaning in this document
ABA	Australian Banking Association
ACCC	Australian Competition and Consumer Commission
AFCA	Australian Financial Complaints Authority
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASIC Act	*Australian Securities and Investments Commission Act 2001*
COBA	Customer Owned Banking Association
consultation paper	*Scams – mandatory industry codes*, released on 30 November 2023
Corporations Act	*Corporations Act 2001*
Criminal Code	*Criminal Code Act 1995*
EDR	external dispute resolution
framework	Scams Code Framework, as defined in the consultation paper
RG 271	ASIC Regulatory Guide 271 *Internal dispute resolution* (RG 271)
IDR	internal dispute resolution
NASC	National Anti-Scam Centre
REP 761	ASIC Report 761 *Scam prevention, detection and response by the four major banks* (REP 761), released on 20 April 2023
Scam-Safe Accord	Australian banks' Scam-Safe Accord launched in November 2023
UK Online Fraud Charter	The Online Fraud Charter in effect in the United Kingdom