KordaMentha

Scams – Mandatory Industry Codes

Response to consultation paper

January 2024

kordamentha.com

Contents

Executive summary 2

Introduction to KordaMentha 3

Key features of the proposed Framework 4

Definitions 6

Obligations 7

Anti-scam strategies 8

Information sharing 9

Consumer reporting, complaints handling, and dispute resolution 10

Sector-specific codes 11

Oversight, enforcement, and non-compliance 12

Contributors 13

Executive summary

KordaMentha welcomes the opportunity to submit input to the consultation on the Proposed Scams Code Framework ('Framework') and industry codes. The views set out in this submission are made on a general basis and limited to the Consultation Paper's scope.

Overall, we support the initiative by Treasury and the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts ('DITRDCA') and acknowledge recent achievements, including:

- Creation of the National Anti-Scam Centre ('NASC') with information sharing and awareness raising progressing well.
- Tactical progress with coordinated website take-downs by the Australian Cyber Security Centre ('ACSC'), Australia Communications and Media Authority ('ACMA') and relevant industry partners.
- Developments with the Australian Bankers Association ('ABA') and Community Owned Banking Association ('COBA') to introduce name checking, scam strategies, and use of biometrics, and manage the speed of payments to high-risk exit channels.
- The existing telecommunications code – *Reducing Scam Calls and Scam Short Messages (SMs) Code* and the success in blocking unwanted messages.

Consistent with the goal of the national cybersecurity strategy to make Australia a global leader by 2030, the Framework provides the opportunity to help consumers and businesses defend themselves against the threats posed by scammers.

We make our submission in support of the Framework. Our input is based on expertise and experience across the financial crime, cybersecurity, forensic, and risk advisory domains, and is provided with the goal of improving the Framework and reducing the threat of scams to Australian consumers and businesses. We see trust in the digital economy, protection of identity credentials, and the promotion of positive mental health outcomes as additional drivers which should be incorporated into the proposed Framework for a holistic and long-lasting approach to combatting scams.

We support participants having anti-scam strategies which are aligned with existing risk management and accountability frameworks. This will reduce complexity, create trust for civil society and other ecosystem participants, and reduce the regulatory burden in already highly regulated sectors. An overarching regulatory framework also provides the opportunity to set clear roles and responsibilities for government, regulators, and industry.

In our view, opportunity exists to leverage existing regulatory frameworks, including the Anti Money Laundering and Counter Terrorism Financing ('AML/CTF') Act and Rules, Financial Accountability Regime ('FAR'), the Prudential Standards, and broader risk management frameworks. The Framework should also incorporate international best practice illustrated by established frameworks (such as those currently applied in Hong Kong and Singapore) and allow for information sharing across borders to ensure continuous improvement in the prevention, disruption, and response to scams.

It will be essential to ensure all sectors that are susceptible to scams – including payments and cryptocurrency businesses – are included from the outset given they already have a central role in key elements of the Framework. It will also be important to extend participation in the Framework to non-Government organisations and representatives of civil society to support an innovative and holistic approach. Our view is that cross-sector codes and mechanisms to enable prioritisation of activities will enhance sector-specific codes to realise the ecosystem concept set out in the Consultation Paper. We support having designated Government leads for certain parts of the Framework and see this as crucial for framework-wide coordination and information sharing which will be a key enabler for success – given the opportunity to empower consumers and businesses to fight against scam threats.

Training and awareness raising efforts should continue, with a focus on providing key materials to enhance consumer and business scam and financial literacy – supporting safe participation in the digital economy.

Overall, KordaMentha welcomes the proposed Framework and looks forward to working with Treasury, DITRDCA, and other stakeholders to include all the elements for success in reducing the harm of scams in Australia. Our response provides suggested improvements to the Framework, and based on our combined experience, we recommend two major priorities are adopted to ensure the foundation is set to create a more robust approach and enhance resilience to scams:

- Leveraging the existing Australian regulatory frameworks.
- Adopting a cross-sector coordination approach, led by the Government through the NASC.

Introduction to KordaMentha

KordaMentha is an independent and trusted advisory firm which provides specialist financial crime, forensic accounting and technology, restructuring, cybersecurity, performance improvement, and real estate services. Our team of over 400 extends across Asia-Pacific and has experience ranging from C-Suite advisory to finance, real estate, and law enforcement. Since 2002, KordaMentha has been entrusted with some of the region's most complex and sensitive commercial situations. We work with clients to solve the challenges facing corporations, financiers, lawyers, private investors, and government clients.

As members of civil society, and a business operating in the digital economy, we are acutely aware of the challenges in understanding and protecting Australia from the threats and ever-growing risks of scams. In particular, our specialist teams below have an active interest in the proposed Framework and industry codes:

- Our Financial Crime Advisory team operates in the Australian and New Zealand markets across a range of sectors providing us with a detailed understanding of the challenges in combatting scams. We have advised Governments as experts in several areas relating to financial crime and understand the importance of having a co-ordinated national response to scams.
- Our Cybersecurity specialists work with boards, executives, and organisations to evaluate risk, develop, and implement risk management strategy, and enhance cybersecurity resilience. We also support clients with their cyber incident response capability. Our experience in cybersecurity provides us with relevant insights in the context of scams, including data governance, information security, and data loss.
- Our Forensic team is one of Asia-Pacific's most trusted, handling complex disputes, investigations, and other critical matters. Our experience with corporate, legal, government, and regulatory clients provides us with insights to assist clients and stakeholders to operate wisely in the scams ecosystem.
- Our Risk Advisory team works with clients to navigate the intricate landscape of risk management. We provide specialised services in Enterprise Risk Management and Operational Risk Management, and conduct risk management, risk change, and transformation initiatives.

As a technologically and politically neutral firm, KordaMentha supports the development of the proposed Framework and related regulation which will offer consistency and alignment with international best practice, clear guidance for sector participants, and transparency for consumers and businesses.

Key features of the proposed Framework

Questions 1–7

Questions 1-7: Key Features of the proposed Framework

We support the proposed Framework and industry codes to enhance Australia's ability to combat scams.

Addressing the harm of scams (question 1)

Building the right levels of support into the Framework from the outset will reduce longer-term costs and regulatory burden. In addition to the sectors currently proposed to be covered by the Framework, we recommend the following considerations should be prioritised:

The mental health of victims and their associates – There is a need for increased support beyond current initiatives on identity security and financial literacy to include consideration of individual and social welfare. Without the right levels of support, costs to Government and the economy will be higher in the future.

Trust in the digital economy by community, business, and Government – Guidance on how to navigate mis- or dis-information in online content should be incorporated into the Framework, including through specific coordination with the Australian Code of Practice and proposed legislation to give enforcement powers to ACMA.

Identity credentials – Recognising how important these are to consumers, and that often a key goal of scams is to obtain personal information which may be misused to open bank accounts, steal money, and facilitate other crimes.

Legislative mechanisms and regulators (question 3), and enforcement of consistent obligations across sectors (question 4)

The Framework should include provisions for cross-sector codes to facilitate the coordination and prioritisation of timing and execution of sector-specific initiatives toward a set of end-state goals to reduce scam activity in Australia:

- A cross-sector approach would leverage existing capability already deployed by banks (e.g. preventative fraud monitoring and detective AML/CTF monitoring) and telecommunication providers (e.g. preventative 'unwanted' caller/messaging).
- A coordinated approach to the protection of, and for, consumers and businesses aligned to an end-state set of goals would assist in creating a robust Framework to make Australia less attractive for scam activity and enhance resilience.

As an example, while the banking sector is focused on delivering capability to identify the payee of financial transactions (assisting the decision at the point of payment instruction by consumers and businesses), the telecommunication and related sectors should take the opportunity to build further preventative capability.

We consider a role for AUSTRAC as key to managing and mitigating scams given its financial crime remit and the transferable value of know-your-customer, transaction monitoring, and other capabilities that reduce the risk of scams. There is also an opportunity to leverage the international cooperation and information sharing networks of AUSTRAC and other financial intelligence units to reduce the risk of scams by acting quickly to stop funds moving into the control of criminals.

The Framework should also incorporate oversight by other regulators, including:

- ACCC – As a lead for consumer interests and to administer the requirements of the proposed expansion of Competition and Consumer Act.
- APRA – Leveraging its responsibility for monitoring risk management standards and the Financial Accountability Regime (FAR), both of which could be extended to explicitly include scams in their scope.
- ASIC – To leverage its responsibility in ensuring board and senior management conduct is appropriate for scam risk management, and related accountability within organisations.
- Office of the Australian Information Commissioner ('OAIC') – To update its existing framework to apply to scams relating to privacy.

Other Government organisations that can and should contribute to the Framework include:

- Australian Federal Police ('AFP') – Having a dedicated scams taskforce to support the Framework, and provide more of a disruptive focus; and
- Australian Signals Directorate ('ASD'), the ACSC, and the Cyber Security Cooperative Research Centre ('CSCRC') – To bring intelligence and response capabilities to detect, disrupt, and prevent scams.

Sectors captured by the Framework (question 5 and 6)

It is our view that the banking pillar of the Framework should be broadened to explicitly include payments businesses. These businesses are closely linked to banking and offer services which are highly susceptible to scams. It is imperative that the Framework be aligned to developments and new capability in the banking and payment sectors from the outset. Not having the same level of preventative measures applied to payments businesses will create vulnerabilities for scammers to exploit and means consumers and businesses will remain the targets of scams.

We also strongly recommend the Framework require participation from its outset by cryptocurrency and crypto-wallet providers as these businesses are often an exit point when scammers seek to move victims' funds. Similar to the rationale for including payments businesses in the Framework, omission of cryptocurrency related businesses would create further vulnerabilities to be exploited by scammers.

Involving the relevant sectors from the outset will:

- Minimise the challenges experienced in other frameworks (e.g. AML/CTF) where introducing new regulatory requirements can take time, playing into the ability of scammers to exploit vulnerabilities in the ecosystem.
- Recognise "Future sectors" reflect the active Australian digital economy participants who can play a significant role in reducing scam impacts.

Having these sectors involved from the outset will also increase intelligence sharing and further reduce the ability of scammers to exploit consumers and businesses.

Structure of the Framework (questions 2 and 7)

Overall, we propose the Framework requires an increased focus on prevention and capability to disrupt scammers and scam related activity rather than to focus merely on the punitive side of non-compliance. This could be addressed by referencing the importance of training and awareness for all stakeholders in the scams ecosystem (scam awareness needs to form part of online safety and financial literacy).

The Framework should also include specific provisions in legislation to provide mandates to:

- Law enforcement (e.g. AFP) and the national intelligence community (e.g. ASD) to consider scams a priority and be able to use their powers and capability accordingly.
- Non-Government organisations (including not-for-profits) and civil society to play an important role in sharing information about the threats posed by scams, and to design and deploy capability to protect consumers, businesses, and trust in the digital economy.

The Consultation Paper does not address liability. As this will be an important topic for all stakeholders, we propose that an approach be developed based on responsibility rather than liability. Responsibilities for each of the stakeholder groups (Government, industry, non-Government organisations, civil society) should be clearly defined and, where possible, existing frameworks governing arrangements should be leveraged rather than new ones created (e.g. data and privacy, and terms and conditions that govern consumer use of services). This approach should include an all-in principle that requires all Framework participants, according to the relevant responsibilities assigned under the Framework and related sector and cross-sector codes, to uphold their role in the ecosystem – representing another opportunity for creating a more robust and effective Framework in Australia.

Definitions

Questions 8–14

Questions 8-14: Definitions

KordaMentha welcomes the proposed definition of scams as a relevant element of the overall Framework, but we propose that it should specifically:

- Reference the harm of diminished trust in the digital economy, and to mental health of potential and actual victims of scams (for the reasons outlined in responses to questions 1-7).
- Recognise that elements of a scam occur, even if it is an unsuccessful attempt to "*...obtain personal information or financial benefit,*" to ensure the widest possible scope to enact the Scam Codes and Framework.

As noted in the Consultation Paper, we agree it is appropriate to differentiate between scams and fraud, and worthwhile to specify that the victims of scams are consumers and businesses.

We also see the benefits of the definition of scams being incorporated in legislation to:

- Define the offences related to a scam.
- Provide a mandate to the sectors, regulators, and government agencies that need to participate in an effective Framework.

Specific to Question 12 (regarding options to address unintended consequences and identify where obligations need to be met by participating businesses), we refer to our responses in relation to:

- Facilitating cross-sector codes and collaboration (as detailed in the response to the framework questions 1-7).
- Providing a mechanism to prioritise and coordinate sector-based activity (also detailed in the response to the framework questions 1-7).

Finally, definitions will also need to recognise the cryptocurrency related business, non-Government organisations and civil society that we recommend be brought into the Framework (refer to responses to the framework questions 1-7).

Obligations

Questions 15–18

Questions 15-18: Obligations

The ecosystem approach to obligations in the Framework is welcomed and includes the supporting elements for success: prevention, detection and disruption, response, and reporting.

To achieve the aims of the Framework, lead responsibility for, and definition of, key elements should be assigned. These include:

- Identifying large-scale or rapidly emerging scam activity. Recognising that an all-in approach is proposed, there should be a lead organisation responsible for the gathering and facilitating the dissemination of information across all Framework participants.
- Handling, mediation, and adjudication of complaint resolution when existing internal and external dispute resolution do not resolve a consumer's or business's issues in sectors included in the Framework (for example, cryptocurrency related businesses – refer responses to questions 1-7 above).
- Definitions, or reference to existing key terms (for example, 'user-friendly' and 'reasonable steps') to ensure clarity and consistency in approach and allow for regulation of core Framework activities.

Further obligations should also be included to address the first part of the definition of scams that relates to "*...obtain[ing] personal information...*" to:

- Ensure the protection of privacy, with information sharing remaining a key principle.
- Mandate that data and cybersecurity standards are a pre-requisite for all Framework participants, and that this forms part of related regulatory and compliance approaches with the opportunity to leverage existing requirements on proposed industry participants.

Anti-scam strategies

Questions 20–25

Questions 20-25: Anti-scam strategies

Consistent with the responses to questions 15-18 relating to obligations, in our view, anti-scam strategies ('Strategies') must form an essential part of each organisation's risk management and accountability frameworks.

The Strategies should be endorsed by accountable persons (e.g. board and senior management) and consideration should be given to assigning clear individual accountability (consistent with frameworks, such as FAR) for scams within organisations. For example, this may be the senior manager responsible for 'the customer' in a bank, telecommunication, or other sector participating in Scam Codes and Framework.

We encourage Strategies adopt a risk-based approach similar to the AML/CTF regime given the large number of industry entities covered by the Framework and the varying size, nature, and complexity of each participant's role and level of scam threats.

Strategies should include measures of success, and consideration should be given to mandating that these metrics form part of an organisation's public reporting requirements under the *Corporations Act*, or similar, depending on the nature of the entity and the sector within which it operates. This transparency will assist with accountability and informing consumers and businesses of the risks and how to protect themselves from scams, including the capabilities developed by their bank, telecommunication, or other service provider(s). Measures of success need to be defined at the Framework level so there is a consistent set of goals against which all participants can align their individual strategies and measure achievement.

Adopting regulatory review of these Strategies would be consistent with the intended risk management and accountability objectives. An option for the review of organisations' Strategies is to consider a model similar to the Anti-Money Laundering program review (under the *AML/CTF Act 2006*) where qualified independent assessment (i.e. not directly by regulators) provides capacity to Government to reach the anticipated high number of participants captured by the Framework.

Further definition of what is required in a program (i.e. enforceable guidelines) would need to be considered as part of the Framework to achieve the intended risk-based approach to developing appropriate Strategies.

Information sharing

Questions 26–29

Questions 26-29: Information sharing

The ecosystem approach to ‘share and use’ are important inclusions in the Framework and provide the basis for effective information sharing – where timely and relevant information will be the single-most critical element in the success of the whole Framework in preventing and disrupting, not just responding to, scam activity.

The Framework should ensure information sharing is directly linked to obligations and compliance for industry participants and is recognised as a core enabler for consumers and businesses to inform and protect themselves.

The role for Government as a lead in facilitating the best information sharing framework to succeed against scams should:

- Promote a ‘share first’ culture (rather than first considering ‘what cannot be shared’).
- Ensure Personal Identifying Information is protected, but in scope of what can be shared (e.g. bank account details, account names, telephone numbers, emails).
- Open the opportunity to non-Government and civil society to provide information sharing capability to Framework participants. Consistent with an ecosystem approach, NASC and AFCX should form part of the information sharing capability. But information sharing should be limited to technology or capability of these entities.
- Recognise and provide for international sharing. This is essential given the transnational nature of scams.

Consumer reporting, complaints handling, and dispute resolution

Questions 30–33

Questions 30-33: Consumer reporting, complaints handling, and dispute resolution

KordaMentha welcomes the proposed approach to complaints handling and dispute resolution. In our view, this is critical for the continued support and interaction between participants.

We encourage a single point of reporting for all consumers and businesses impacted by scams. Currently, victims may be asked by a bank or other sector participants to report to them, state/territory police, and either Scamwatch or the ACSC. A single data collection point for consumers and business would simplify the process and reduce the stress on victims of scams, as well as assist in promoting positive mental health outcomes from exposure to scams. It also creates the opportunity to provide case updates to victims and create a single point of capture to enable real-time data sharing, education activities, communications across the ecosystem, and timely prevention initiatives.

Sector-specific codes

Questions 34–42

Questions 34-42: Sector-specific codes

Similar to our responses to questions 1-7 relating to legislative mechanisms and regulators, and enforcement of consistent obligations across sectors, we suggest that cross-sector codes and mechanisms (in addition to sector codes) be established to prioritise and coordinate actions.

To ensure industry codes are updated on an ongoing basis, Government should continue to engage with industry and civil associations and share data-led intelligence to help identify and design solutions to prevent, detect, disrupt, respond to, and report scams.

Oversight, enforcement, and non-compliance

Questions 43-45

Questions 43-45: Oversight, enforcement, and non-compliance

We support the role for regulation and imposition of penalties for non-compliance, given the serious nature of, and threats posed by, scams to the digital economy and diminished trust of consumers, among the other harms identified in our response to questions 1-7.

We suggest consideration be given to an over-arching coordination agency to govern the multi-regulator approach to scams and the obligations under this Framework. This would help avoid duplication and leverage existing capabilities, with particular consideration given to:

- Applying the current financial crime framework (including the public-private partnership – Fintel Alliance) to assist in cooperation and information sharing.
- The establishment of a coordinating body for scams similar to the e-safety commissioner.

We encourage Government to consider adopting different approaches to enforcement (e.g. 'Smarter Regulation') as an important step in completing a Regulatory Impact Assessment.

Smarter Regulation enables those participants who are lower risk and can demonstrate through reporting that they have detected scams and prevented losses to experience a lesser level of regulatory scrutiny. Those participants who put in place fewer controls resulting in higher incidents of scams would be more likely to be the focus of regulatory attention under this approach.

In addition, initiatives such as independent audits of Strategies (as referenced in response to Questions 20-25) would assist in supporting regulatory capacity for oversight and provide the necessary assurances to Government agencies in relation to compliance with the Framework.

An innovative regulatory approach can provide the foundation for creating trust in the ecosystem and provide the platform to support public confidence in the digital economy.

Contributors

Key contributing authors

Rachel Waldren
Partner

Anya Gielen
Executive Director

Guillaume Noé
Executive Director

KordaMentha

Contact us

Auckland
+64 9976 4747

Brisbane
+61 7 3338 0222

Jakarta
+62 21 3972 7000

Melbourne
+61 3 8623 3333

New Zealand
+64 9976 4747

Perth
+61 8 9220 9333

Singapore
+65 6593 9333

Sydney
+61 2 8257 3000

Townsville
+61 7 4724 9888

For more information visit
kordamentha.com