Scams Taskforce,

Market Conduct and Digital Division,

The Treasury,

Australia Government.

28 January 2024

Subject: Response to “Scams – Mandatory Industry Codes” Consultation Paper.

Dear Sirs,

Tanla Platforms Limited, recognized as a Visionary in the 2023 Gartner® Magic Quadrant™ for Communications Platform as a Service (CPaaS), is pleased to offer this response to the Consultation Paper on “Scams – Mandatory Industry Codes.

Our submission is based on the experience we’ve gained in developing, proving and deploying an anti-phishing solution in India.

We are grateful for the opportunity to contribute to this policy discussion and look forward to further engagement on these topics.

Yours sincerely,

Sd/-

Sunil Bajpai

Chief Trust Officer, Tanla Platforms Limited.

Former Principal Advisor, TRAI.

List of stakeholder questions

Questions on the proposed Framework

1. **Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?**

   Yes, the Framework does address the harm of scams. The initial designated sectors and the proposed obligations align well with the objective of combating scams.

   In addition to these measures, it may be beneficial to include Internet Service Providers (ISPs) and takedown agencies in the initial phase of the regulation:

   - ISPs can effectively block malicious URLs by manipulating DNS responses or filtering data packets.
   - Bringing takedown agencies and services under regulation can remove legal uncertainties, establish a predictable process, and thus improve the response time and effectiveness of such services.

2. **Is the structure of the Framework workable – can it be implemented in an efficient manner? Are there other options for how a Framework could be structured that would provide a more efficient outcome?**

   Yes, the framework's structure addresses critical areas and mechanisms necessary to organise effective countermeasures against scam activities.

   Scammers operate in a manner that makes them hard to trace or identify. They quickly exploit a victim's lack of awareness or vulnerability and then disappear, after erasing their footprints. This requires ***adoption of technological measures*** in prevention, coordination of counterstrike and support to law enforcement agencies to identify and punish the wrong doers, thereby minimizing the recurrence, in line with the proposed Framework.

   The framework could, therefore, encourage development and adoption of RegTech, by requiring the regulators to evaluate this option while creating their sector-specific codes.

   More comments are offered against specific questions in the consultation paper.

3. **Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?**

   The success of the Framework hinges on legislative mechanisms being aligned with the desired outcomes, particularly in sectors that heavily rely on communication systems: like banking and, potentially in the future, e-commerce.

   One effective approach could be the incorporation of ***strict liability*** within the legal framework. If a scam could reasonably have been prevented through pre-emptive measures, businesses that failed to implement adequate technological solutions or safety practices would be held responsible for compensating loss.

   What is deemed 'adequate' preventative measures should be expected to evolve in response to the changing tactics employed by scammers and advancements in anti-scam technologies.

4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?

Yes, the Framework does establish foundational mechanisms for enforcing consistent obligations across sectors.

For it to be truly effective, the regulators' role is important in adapting it to different sectoral needs, bringing clarity and practicality in the codes and guidelines. Plus, the regulators have the important role of effective enforcement.

5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?

Yes, the framework is sufficiently flexible to enable swift inclusion of additional sectors where new scams are detected.

Sector-specific regulators should be expected to act pre-emptively, preparing in advance to effectively confront and address scam activities as they emerge in their respective domains. This proactive stance would ensure that the framework remains relevant and robust, even as scam tactics and target sectors evolve.

6. What future sectors should be designated and brought under the Framework?

In addition to the sectors currently covered, it's important to consider expanding the Framework to include others as the landscape of scams evolves:

- e-Commerce and Retail: Given the high volume of online transactions and the personal data involved, these sectors including the sectors that support the retail and e-commerce such as courier services etc., are increasingly becoming targets for sophisticated scamming activities.
- Gaming: With the rise of in-game purchases and virtual economies, the gaming industry is becoming more susceptible to various forms of online fraud and scams.
- Healthcare, Travel, and Hospitality: These sectors deal with substantial personal and financial information, making them attractive targets for scammers.
- Education: With the increasing digitization of educational resources and services, this sector could face unique scamming threats, such as fraudulent educational platforms or scholarship scams.
- Government and Public Services: As these services increasingly move online, they become potential targets for scams designed to mislead or defraud citizens. Government communications also have built-in penalty if you disregard them, making citizens likely to fall a prey to the scammers.

7. What impacts should the Government consider in deciding a final structure of the Framework?

In finalizing the Framework's structure, the government should assess how various components either strengthen or weaken ***incentives for prompt action*** against scams.

For instance, the takedown of scam websites usually happens too slowly to affect the scammers, who remove their own sites within days, if not hours, to evade detection and traceback to them. A more efficient approach might be to focus on early detection and blocking of malicious links in messages or collaborating with internet access providers and DNS servers to inhibit access to harmful URLs, which can be quicker than the existing legal takedown process.

Introducing strict liability, as suggested in response to question 3, promotes discovery of "what works?". It encourages proactive discovery and implementation of effective strategies, as businesses would have a ***direct incentive to prevent scams*** to avoid liability, instead of solely focussing on compliance with laws or regulations.

Another aspect to consider is the ***standard of KYC*** and the ***protection of user data*** in each sector. Robust KYC can ensure that telecom resources are not misused for fraudulent activities. Similarly, KYC that meets specified standards for other sectors would prevent initiation or completion of fraud in that sector. Same holds for data protection.

The government should consider the potential impacts of each element of the Framework on the incentive for speed and effectiveness of anti-scam actions, in addition to the overall compliance environment for businesses.

Questions on definitions

8. Is maintaining alignment between the definition of 'scam' and 'fraud' appropriate, and are there any unintended consequences of this approach that the Government should consider?

Yes, maintaining alignment between the two is appropriate.

Furthermore, leaving the actual development of the codes and regulations to sector regulators, as is proposed, automatically should take care of unintended consequences.

9. Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?

Yes, it is a good definition to use.

10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?

Yes.

11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?

In legislating the definition of a scam, the primary impact to consider, arises from the adaptability of scammers. A narrow definition of scam could allow scammers to escape the law.

A related impact is the potential for businesses to evade responsibility. A well-crafted definition should ensure that businesses cannot avoid accountability by exploiting ambiguities. It should delineate their obligations in preventing, identifying, and responding to scams.

Additionally, the definition's impact on sector-specific nuances is important. While a general framework provides an overarching definition, sector-specific codes are necessary to address unique fraudulent practices for respective sectors. This approach ensures that the definition is sufficiently flexible to adapt to the specific challenges and risks each sector faces.

Therefore, the legislative definition should remain inclusive enough to cover evolving scam tactics. As already proposed in the consultation, "sector-specific codes could provide further guidance on the meaning of 'scams' based on specific fraudulent practices observed in each sector…". This dual approach of a general framework supported by sector-specific details combines the necessary breadth with the depth required for effective scam prevention and enforcement.

12. Will the proposed definitions for designated sectors result in any unintended consequences for businesses that could not, or should not, be required to meet the obligations set out within the Framework and sector-specific codes?

No.

13. **Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?**

Defining the sectors captured by the Framework in the primary law would be the more effective approach:

Consistency and Clarity: Including sector definitions in the primary law ensures a consistent and clear understanding of each sector's scope and responsibilities, thus avoiding overlap or conflict.

Legal Authority: Definitions included in primary legislation carry legal authority, whereas industry-specific codes would need to trace the authority to the primary legislation, sectoral laws, or license conditions. This may not always be easily possible.

The unique characteristics and needs of each sector can, of course, be addressed in their respective codes.

14. **What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?**

When defining digital communications platforms for the Framework, it's crucial to consider the diverse ways platforms are used, which may extend beyond their primary function.

For instance, gaming platforms, though not primarily classified as "connective media services," enable user interactions and often involve financial transactions. The anonymity of participants and the immersive nature of games create an environment conducive to scams. These characteristics provide a fertile ground for a scamster disguised as a fellow gamer to make a "dishonest invitation, request, notification or offer, designed to obtain personal information or financial benefit by deceptive means".

Similarly, 'connective media services' that offer end-to-end encryption uphold privacy and freedom of expression, yet this feature can inadvertently provide a haven for scammers, particularly as these platforms begin to incorporate payment services or commercial communications. In this context, the government should consider legal provisions that enhance the liability of such platforms for scams that occur through their services, regardless of the platform providers' direct involvement or culpability.

The Framework should extend to include all digital applications that involve commercial activities, payments, or conversations. This extension is essential to encompass a broader range of platforms where scams might occur, reflecting the ever-evolving digital landscape. By broadening the definition in this manner, the government can ensure that the Framework remains effective and relevant in addressing the risks associated with modern digital communication and transaction platforms.

Questions on overarching principles-based obligations

15. **Are there additional overarching obligations the Government should consider for the Framework?**

No comments.

16. **Are the obligations set at the right level and are there areas that would benefit from greater specificity e.g., required timeframes for taking a specific action or length of time for scam-related record-keeping?**

Yes, the obligations are set at the right level. Sectoral codes may provide greater specificity, where needed.

17. **Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?**

The overarching obligations outlined in the Framework are not seen to be detrimental to either businesses or the consumers they serve.

In fact, these obligations are likely to form and strengthen the trust between business entities and consumers, which is critical for maintaining and growing a loyal customer base in the modern, digital-first economy.

Therefore, these obligations interact positively with business objectives, particularly those concerning the provision of efficient and safe services to consumers.

18. **Are there opportunities to minimise the burden of any reporting obligations on businesses, such as by ensuring the same information can be shared once with multiple entities?**

Yes.

Regulations should enable exchange of information through an interoperable system. A blockchain based exchange (permissioned distributed ledger) has been developed by Tanla Platforms that allows stakeholders to create immutable and non-repudiable records of actions, which can be accessed by relevant participants based on their privileges or upon satisfaction of pre-conditions.

This allows reliable, efficient and immediate sharing of information.

19. **What changes could businesses be expected to make to meet these obligations, and what would be the estimated regulatory cost associated with these changes?**

To comply with these obligations, businesses may need to implement small adjustments. The associated regulatory costs would be far lower than financial losses resulting from scams. These losses not only have a monetary impact but also risk eroding consumer trust in communication and digital platforms. Therefore, the investment required for these changes is likely to be a fraction of the costs incurred due to ongoing scam activities.

The changes required by businesses would be minimal and the cost of regulatory burden would be a tiny fraction of the losses that occur today, and which threaten to undermine trust in communication and digital platforms.

Questions on anti-scams strategy obligation

20. **What additional resources would be required for establishing and maintaining an anti-scam strategy?**

It could be a part of the risk management function in the businesses, with some supplementary resources.

21. **Are there any other processes or reporting requirements the Government should consider?**

The government should consider mandating businesses to publicly disclose their anti-scam measures to the greatest extent possible. Far from being a regulatory burden, this requirement can serve as an opportunity for businesses to distinguish themselves from competitors by demonstrating their commitment to scam prevention.

Such disclosures should detail how the business adheres to specific sector codes and reveal their performance based on relevant metrics. These could include the number of scam-related complaints received in relation to the volume of transactions or the number of consumers they serve. Defining

these metrics within the sectoral codes would standardize reporting and provide a clearer picture of a business's effectiveness in combating scams. This approach not only enhances transparency but also promotes consumer trust and industry accountability.

22. Are there parts of a business's anti-scam strategy that should be made public, for example, commitments to consumers that provides consumers an understanding of their rights?

Publishing elements of a business's anti-scam strategy, particularly those relating to consumer rights and protections, would be beneficial.

This transparency not only reassures consumers about the safety measures in place but also motivates businesses to adopt and rigorously implement effective anti-scam practices. Making these commitments public demonstrates a business's dedication to consumer safety, fostering trust and accountability in the business-consumer relationship.

23. How often should businesses be required to review their anti-scam strategies and should this be legislated?

Businesses should be obligated to continually evaluate their anti-scam strategies based on specific, quantifiable metrics outlined in the relevant sectoral codes, as well as any additional standards they publicly commit to their customers.

The exact frequency of these reviews may be determined by the guidelines set within these sectoral codes. However, businesses should be encouraged to conduct these evaluations more frequently if they face serious scam-related challenges or if they voluntarily choose to adopt a more rigorous review schedule. This approach allows for flexibility while ensuring that anti-scam measures remain effective and responsive to evolving threats.

24. Are there any reasons why the anti-scams strategy should not be signed off by the highest level of governance within a business? If not, what level would be appropriate?

The anti-scams strategy should indeed be signed off at the highest level of governance within a business, such as the Board of Directors or the CEO. This level of oversight would ensure that the strategy receives the necessary attention and resources, demonstrating a strong commitment to combating scams. It would also align the strategy with the organisation's overall goals and risk management policies.

Additionally, it should be mandated that the performance and effectiveness of the anti-scams strategy be reviewed at the same level at which it was approved. This assessment should be made at least annually.

Such a process not only reinforces accountability but also ensures that the anti-scam measures remain relevant and effective over time.

25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?

Regulators should play a proactive and collaborative role in guiding businesses to develop compliant anti-scam strategies. This involves not only defining and establishing sector-specific codes but also actively engaging in consultations with all relevant stakeholders, such as the businesses themselves, consumer groups, legal experts, and technology specialists. The aim of this engagement should be to ensure that the codes are comprehensive, practical, and reflective of the current scam landscape.

Furthermore, regulators should define periodic, standardised reporting requirements for responsible businesses in the sector. These reports may be published to inform all stakeholders about the effectiveness of the anti-scam measures.

This level of ongoing engagement is essential to ensure that anti-scam strategies remain robust, adaptable, and in line with evolving scam methodologies and technologies.

Questions on information sharing requirements

26. What resources would be required for establishing and maintaining additional information sharing arrangements with other businesses, the NASC and sector-specific regulators under the Framework?

To enhance information sharing among businesses, the NASC, and sector-specific regulators under the Framework, the establishment of a scam information exchange utilizing permissioned distributed ledger technology (DLT) could be highly effective.

This approach has been successfully implemented by Tanla Platforms in the telecom sector in India and offers several advantages:

(i) Business or other agencies can act on information available with them and create reports or alerts, as needed for others. Their actions remain traceable to them, and the records cannot be tampered with.

(ii) The distributed nature of this system means that the infrastructure is maintained by the ecosystem participants themselves, reducing the need for significant government or regulatory resources. Each participant, or 'node', contributes to the overall infrastructure, making the development and maintenance of this system a shared responsibility and cost.

(iii) The design of the exchange can incorporate rules that determine who can access specific types of information. This can be based on the roles of the participants or enforced through smart contracts. Such a structured approach ensures that relevant parties have access to the necessary data, while also upholding privacy and security requirements.

27. What safeguards and/or limitations (regulatory, technical, logistical or administrative) should the Government consider regarding the sharing of information between businesses, the NASC or sector-specific regulators?

It may be expected that the scope of information sharing would expand over time to encompass a broader range of scams and sectors. Stakeholders within these sectors, it may be hoped, would also begin to engage more proactively because of these measures. Therefore, safeguard and/or limitations would need to evolve in tandem with these demands.

While regulatory safeguards are debated to define the boundaries of permissible information sharing, technical security measures must be considered for their actual implementation. A DLT based exchange suggested above can effectively ensure data integrity and confidentiality, preventing unauthorised access.

28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?

Please see response to Question 27.

29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?

One major impediment to the sharing of intelligence is the risk of false positives, which could be strategically triggered by scammers to overwhelm systems that receive the alerts. The false alarms can lead to the diversion of resources towards addressing non-existent threats, thereby diluting the

effectiveness of the system in responding to genuine scams. To mitigate this, robust verification protocols are needed before creating or acting on an alert. Additionally, participation in the intelligence-sharing ecosystem should be limited to reliable stakeholders.

Secondly, there are concerns related to inadvertent sharing of personal communication that is misclassified as a scam. This would require safeguards contingent upon the threat level under different conditions. An example of the safeguard could be to require reporting to law enforcement first, who may then choose to release the information to other stakeholders.

Finally, there is risk of data breach in organisations with whom sensitive information is shared by businesses. Regulators can impose obligations on recipient organisations that must be fulfilled before they can seek information from other service providers or government agencies.

Questions on consumer reports, complaints handling and dispute resolution

30. What are the limitations or gaps that need to be considered in leveraging existing IDR requirements and EDR schemes for the purposes of this Framework?

No comments.

31. If the remit for existing EDR schemes is expanded for complaints in relation to this Framework:

a. what criteria should be considered in relation to apportioning responsibility across businesses in different sectors?

Responsibility for compensating losses should be clearly delineated, either by specific laws or sectoral regulations. For instance, in the case of an OTP scam resulting in fraudulent debits, the banking sector, which benefits from the efficiency of digital banking, should be primarily responsible for compensating the victim. This is because the delivery of OTPs by SMS is a decision made by the banking sector. However, telecom companies may hold some responsibility, such as in cases of spoofing or failure to detect scam messages. This liability could be contractually transferred between the bank and the telecom company, allowing banks to negotiate solutions with telecom providers and telecom companies to set competitive prices for their services, factoring in the cost of potential liabilities.

b. how should the different EDR schemes operate to ensure consumers are not referred back and forth?

To prevent consumers from being caught in a back-and-forth between sectors, the EDR mechanism designated for the primary sector implicated in the scam should resolve disputes between the business and the consumer. If another sector is found culpable through the EDR process, any liability transfer should adhere to existing contracts between the businesses. This ensures that consumers have a clear, direct path for dispute resolution without being shuffled between different sectors.

c. what impacts would this have on your business or sector?

For a company like Tanla Platforms, which provides anti-phishing solutions and other services to telecom companies, this proposed regime would create an environment where the company competes based on the performance of its products and platforms. For instance, the effectiveness and reliability of its anti-phishing solutions would be key in securing contracts with telecom companies, which would be more incentivized to invest in robust scam prevention technologies due to their potential liability.

32. **Should the Government consider establishing compensation caps for EDR mechanisms across different sectors regulated by the Framework? Should these be equal across all sectors and how should they be set?**

Compensation caps for EDR mechanisms in different sectors need to be tailored to the specific risks and transactional values characteristic of each sector. A one-size-fits-all approach may not be appropriate given the diverse nature of transactions and the varying degrees of risk across different sectors.

Setting the caps would require a careful analysis of historical scam data, average transaction values, and the potential impact of scams in each sector. Regular reviews and adjustments might be necessary to ensure that the caps remain relevant and effective in light of changing market dynamics and scamming techniques. The market price is the best mechanism to provide adequate protection to businesses and consumers alike.

Therefore, compensation caps should be determined based on sector-specific regulations or be spelt out in contracts with consumers.

33. **Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?**

Yes.

Questions on sector-specific codes

34. **Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?**

Yes.

35. **Are there additional obligations the Government should consider regarding the individual sector codes?**

To develop the sector codes may be left to the sector regulators or to the relevant government agencies responsible for governing the sector.

36. **Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?**

Yes.

37. **Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?**

Yes.

38. **Are the proposed approaches to developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?**

Yes. Sector-specific codes are an appropriate approach for meeting the objectives of this Framework.

All codes should be required to declare their own effectiveness metrics and identify the agency that would review and published the results at a defined periodicity.

39. **Should any of the proposed sector-specific obligations specify a timeframe for a business to take action, and if so, what timeframe would be appropriate?**

The decision on whether to specify timeframes for sector-specific obligations and what those timeframes should be is best left to the discretion of the sector regulator or other authorities overseeing the development of the code. They are better positioned to understand the nuances and operational realities of each sector and can set realistic and effective timeframes accordingly.

40. **What changes could businesses be expected to make to meet the sector-specific code obligations, and what would be the estimated cost associated with these changes?**

This can only be commented upon when the codes are fully in place and operational. For the three initial sectors that have been identified, this cost should not be consequential.

41. **What are the relative costs and benefits of other available options, pathways or mechanisms, such as co-regulation, to set out additional mandatory sector-specific obligations?**

Co-regulation is a good option that sector regulators can adopt. It provides the flexibility necessary for a nimble response to changing threats.

However, co-regulation is only suitable where there are a few participants or the sector is well organised with its own industry body. Even then it requires a strong regulator to guide the process. Possibility of adopting appropriate RegTech is also a big factor of success.

Unlicensed and monopolistic (or oligopolistic sectors) may be most resistant to co-regulation because would have a tendency to use the process to their own advantage. This can be prevented by bringing in legal provisions to define the obligations and provide for enforcement.

42. **Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?**

No comments.

Questions on approach to oversight, enforcement and non-compliance

43. **How would multi-regulator oversight impact different industries within the scams ecosystem? Are there any risks or additional costs for businesses associated with having multi-regulator oversight for enforcing the Framework?**

With clear responsibilities in their own sectors, a multi-regulator oversight is not expected to present too many problems. The regulators may be relied upon to coordinate the work in such a way that allows the business to operate without undue burdens.

44. **Are there other factors the Government should consider to ensure a consistent enforcement approach?**

No comments.

45. **Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?**

The penalties may not be equal across all sectors, but uniform principles could be set down in law to guide the sector regulators to ascertain appropriate penalties for such breach.