genpact

Scams – Mandatory Industry Codes

Genpact Response to Consultation

January 2024

Table of Contents

1. Introduction

We welcome the opportunity to respond and provide feedback on The Treasury Australian Government consultation paper Scams – Mandatory Industry codes.

The need for a co-ordinated approach in Australia is vital, with losses to Australians increasing exponentially over the last decade. The impact on individuals, families and businesses can in most cases be crippling. The need for accountability and regulation in the payments eco-system is critical in combatting the impact of scams.

The proposed ecosystem-wide obligations within the consultation paper are well known practices in the Financial Industry. The consistency of the robustness and execution of these practices across the ecosystem is critical to the success of any co-ordinated intervention.

2. Response to Consultation

Detailed below are our responses to the consultation paper on Scams – Mandatory Industry Codes issued by the Treasury and the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA).

Our responses are informed by experts within our Financial Crime Risk Management practice and include our learnings and experience with numerous clients within and outside Australia.

2.1 Proposed Scams Framework

Question	Genpact Response
1. Does the Framework appropriately address the harm of scams, considering the initial designated sectors and the proposed obligations outlined later in this paper?	The framework currently does not consider non-deposit taking financial institutions and insurance companies. Service providers such as Utilities providers, Post and courier service providers and Toll management companies are also not covered under the proposed framework but are consistent targets of scams
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?	While the approach of drafting sector specific codes is well received, scams are multidimensional and should be tackled across not just sector but also jurisdictions (international vs domestic and countries with appropriate co-operation regimes or otherwise) and the type of scam (digital vs face-to-face)
3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?	While each sector has a regulator supervising scam response management, scams that span across more than one sector would require co-operation across sectors. For example, payments to a bank account initiated through a telecommunication-based scam. An overarching data sharing and collaboration framework preferably through a central entity (similar to an FIU) could help address this requirement.
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?	With the appropriate amendment to regulation, regulators will need to be appropriately resourced and trained to audit performance, enabling enforcement agencies to effectively ensure compliance
5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future	While future sector additions are included in the framework, specific sectors that are already impacted substantially by scams but not included in the sectors currently proposed should be, in our opinion, factored into the current regulatory uplift

6. What future sectors should be designated and brought under the Framework?	Utility companies (gas, electricity etc.), Australia Post and other courier services, Toll management companies. We believe these sectors require urgent regulatory uplift related to scams and are best served in the current exercise rather than being marked for future expansion
7. What impacts should the Government consider in deciding a final structure of the Framework?	

2.2 Definitions

Question	Genpact Response
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?	
9. Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?	We suggest the inclusion of communication which, in the light of circumstances under which they were made, require specific disclosures for an informed decision/action and where such disclosure is wilfully withheld with intent to deceive
10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?	While the proposed definition considers the theft of "personal information" which includes sensitive information and credit information, the definition of "personal information" under the Privacy Act 1988 does not include the personal information of someone who has died. Scams used to obtain personal information (especially sensitive information) of deceased loved one can be used to victimise individuals
11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?	Several scam perpetrators already have an international footprint requiring Australian authorities to work with international agencies to effectively disrupt scam activity. Ensuring the definition of a scam is aligned across these international agencies will enable smoother co-operation.
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?	
13. Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?	Detailed definitions may be included in the industry specific codes with the primary law, making references to these
14. What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?	Financial institutions other than ADIs should also, in our opinion, be included. These would encompass insurance companies, lending institutions that do not take deposits, money service/transfer businesses, digital currency exchanges.

2.3 Principles Based Obligations

Question	Genpact Response
15. Are there additional overarching obligations the Government should consider for the Framework?	Implementation of an audit regime on an established frequency is essential to ensure the scam strategy, coverage across new and existing products and services, new customer types/profiles are currently adequate and continue to be adequate in the face of changing scam typologies. Principle based obligations, in our opinion, should also include the obligation to co-operate with local and international organisations (both private and public) to the extent allowed by local laws (such as privacy law)
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?	Specifics may be tailored to the nuances of each sector in the sector level codes rather than inclusion in the principle-based obligations
17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of 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?	In the instance where a cross sectoral scam has been identified or a scam impacting more than one organisation, it is suggested to allow for the reporting entity to grant access to other impacted entities allowing them to add in additional information to the same incident without needing to create additional scam reports. This will also allow the regulators to access all relevant information related to a specific cross sectoral or multi-entity scam in a single comprehensive report and reduce the reporting burden for reporting entities
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?	Developing and maintaining a frictionless, efficient, and transparent system that allows consumers to raise scam incidents and obtain ongoing updates on resolution status requires a substantial commitment from organisations in terms of trained human resources. Banks currently already struggle with dispute resolution backlogs with available resourcing. Sufficiently staffed scam management operations can be expected to increase operational costs either through direct or outsourced resourcing

2.4 Anti-Scam Strategy

Question	Genpact Response
20. What additional resources would be required for establishing and maintaining an anti-scam strategy?	In order to ensure organisations are able to create anti-scam strategies that meet minimum industry standards, the sector level codes may provide details on necessary inclusions that organisations should consider along with indicative detail on specific common products or services within that sector.
21. Are there any other processes or reporting requirements the Government should consider?	Mandated audits of the anti-scam strategy, at a minimum frequency (such as annually) will ensure the strategy is relevant and consistently updated taking into consideration changes to products, services, customer segment and scam approaches.

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?	While the sharing of aspects of the anti-scam strategy with consumers should remain specific to the rights and obligations of the consumer, organisations within a sector should be encouraged to share their anti-scam strategy in entirety amongst themselves to enable each other to further enhance their approach leading to widely implemented industry best practices
23. How often should businesses be required to review their anti-scam strategies, and should this be legislated?	Businesses should be required to update their anti-scam strategies every time a new product, service, jurisdiction, or customer type is serviced. An annual review should be legislated to ensure any changes to the scam environment is appropriately considered within the anti-scam strategy
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?	We believe the impact of scams on consumers and the economy is substantial enough to warrant oversight and sign off of the anti-scam strategy at the level of the board.
25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?	With businesses developing their own anti-scam strategies, processes and controls, regulator support in enabling the sharing of best practices across businesses, ongoing publishing of guidance notes on scam findings and inadequacies identified within businesses as well as product, service, or jurisdiction level guidance on anti-scam strategies.

2.5 Information Sharing Requirements

Question	Genpact Response
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?	Businesses would benefit with guidance around the specific data elements that are to be reported on, in relation to a scam, that will be required by other impacted businesses within and outside a sector.
27. What safeguards and/or limitations (regulatory, technical, logistical or administrative) should the Government consider	The security framework of the data sharing platform is of paramount importance to ensure sensitive information is not made available to unintended parties. An effective participant identification process is also essential to ensure that businesses seeking access to the platform and their designated representatives are appropriately vetted and are who they say they are before being granted access to scam incident data.
28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?	
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?	Businesses are required to ensure that any information shared does not contravene the requirements of any existing laws (local and international) that the business is subject to. This may cause organisations to de-risk completely or take an extremely conservative approach impacting the amount of valuable information that is shared. To encourage and enable quicker sharing of information, guidance may be provided to businesses on specific information sharing legislation applicable locally and for multi-national organisations subject to legislation from major foreign markets.

2.6 Consumer reports, complaints handling and dispute resolution.

Question	Genpact Response
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?	Resourcing available to EDR schemes will need to be reviewed to ensure additional dispute resolution responsibilities can be adequately managed in a timely manner. AFCA is already faced with an unsustainable increase in complaints.
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? b) how should the different EDR schemes operate to ensure consumers are not referred back and forth? c) what impacts would this have on your business or sector?	a) Responsibility allocated in each instance would depend on the nature of the scam, parties involved and their role, the specific product/service, jurisdictions involved and the circumstances of the case. We believe it would not be possible for legislation to pre-empt all scenarios although sector specific codes may contain broad guidelines and certain case specific examples. b) We suggest an approach where the initiator of the complaint/dispute is not required to follow up with other parties once the EDR process is initiated except to provide information requested by the impacted business or regulator. This will require the regulator to be sufficiently staffed to manage all ongoing communication with all relevant parties directly until the dispute is resolved. c) Improving the ease of reporting scams will result in an increase in volume of scam reports and disputes both to businesses and regulators. Businesses will need to invest in both technology and human resources to be able to manage the increased volumes in a timely manner.
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?	With the increasing complexity and frequency of scams, and the need to ensure consumers and businesses are adequately protected, we believe a cap on compensation would not be a fair and just approach. A large financial scam loss to a consumer should warrant the direction of more resources to compensate/protect the consumer than a set cap. We do believe that the process for determining compensation in each scenario will need to be robust and transparent to ensure financial resources are not poorly applied. In regard to sector specific compensation, we believe caps should not apply and specific compensation amounts be determined on a case-by-case basis while adhering to broad compensation guidelines.
33. Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?	We believe the framework does provide a clear pathway for compensation to consumers.

2.7 Sector specific codes

Question	Genpact Response
34. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?	We subscribe to the need for sector specific obligations to enable legislation to effectively cover sectoral nuances for the protection of customers and for providing businesses with the flexibility they need.

35. Are there additional obligations the Government should consider regarding the individual sector codes?	Along the lines of banks providing an indicative validation of BSB and Account number with respect to a payee name, it is suggested that telecommunication providers enable an indicative notification of whether a link provided in a message could potentially be related to a scam.
36. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?	
37. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?	
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?	
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?	We believe that it is imperative to specify timeframes for specific obligations. Specific suggestions are mentioned below: 1. Dispute resolution – 60 days 2. Sharing of scam information with regulator/other providers- As early as possible subject to a maximum of 5 days 3. Blocking a scam phone number/message header – 5 days 4. Initiate investigations on notified scams within 10 days 5. Timelines for report submissions to the regulator
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?	We believe improved and frictionless scam reporting capabilities provided to consumers are likely to increase the volume of scam reports requiring manual review, validation and investigation which will require a greater investment in technology and trainer human resources.
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?	
42. Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?	

2.8 Approach to oversight, enforcement, and non-compliance

Question	Genpact Response
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?	We believe multi-regulator oversight on a single sector will result in delays in dispute resolution and complications in being able to conduct supervisory responsibilities. These can be avoided by centralising supervisory responsibilities with a single regulator for each sector. The proposal to expand the supervisory responsibilities of existing regulators over their sector, such as with

	ASIC in banking, is a welcome approach likely to function effectively.
44. Are there other factors the Government should consider to ensure a consistent enforcement approach?	With a single regulator per sector, it will be imperative for these regulators to have guidelines for co-operation to effectively manage multi-sector scams.
45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?	We believe uniform and equal penalties across sectors will ensure no sector is unduly penalised over the other.

3. Key Authors and Contributors

Brian Baral
Senior Vice President, Banking and Capital Markets

Quinten Hout
Vice President, Financial Crime Risk Management Advisory

Brett Jones
Vice President, Financial Crime Risk Management

Shaurya Sharma
Vice President, Consulting

About Genpact

Genpact (NYSE: G) is a global professional services firm that makes business transformation real. We drive digital-led innovation and digitally-enabled intelligent operations for our clients, guided by our experience running thousands of processes for hundreds of Global Fortune 500 companies. We think with design, dream in digital, and solve problems with data and analytics. We obsess over operations and focus on the details – all 78,000+ of us. From New York to New Delhi and more than 20 countries in between, Genpact has the end-to-end expertise to connect every dot, reimagine every process, and reinvent companies' ways of working. We know that rethinking each step from start to finish will create better business outcomes.

For additional information contact Brett Jones, Vice President, Financial Crime Risk Management *brett.jones@genpact.com*.