Scams
Mandatory Industry Codes

Consultation paper

BioCatch Response
January 2024

Reference:
https://treasury.gov.au/consultation/c2023-464732

Table of Contents

Attention: Scams Taskforce

Thank you for the opportunity to consult and respond to the Scams Consultation paper. We believe this is a fantastic initiative by the Australian government and will provide transformational benefits in how citizens and businesses are impacted by scams.

Our company is a global technology provider that has dedicated the past twelve years to helping organisations detect digital fraud and scams. As of December 2023, BioCatch profiles over 8.5 billion digital sessions per month, which allows us to gain a deep insight into the dynamics of global scam and fraud activity.

Executive Summary

The key objective of the Scams Consultation paper is to gather inputs that will help define a 'regulatory framework that sets clear roles and responsibilities for the Government, regulators, and the private sector in addressing scams'. The desired outcomes are essentially to reduce the financial, emotional, and behavioural impacts of scams against the citizens of Australia.

In preparing our response, we have used these principles as the starting point and a guideline for the feedback submitted. By implementing these elements into the Framework, our belief is that these specific outcomes may be achieved:

- Stabilising scam losses in the first year of the framework.
- Reducing the $3.1 billion baseline from year two and beyond by over 50%.
- Maintaining trust in the banking, telecommunications, and digital communication platforms.
- Provide clear obligations to the impacted organisations, so investment and resources may be allocated accordingly.
- Increasing transparency of financial impacts and progress against fighting scams.
- Maintain flexibility, to respond to future scam types and trends.
- Implementation of controls that do not impede innovation and growth in digital services.
- Simultaneously disrupt adjacent forms of financial crime such as drug trafficking, human trafficking, and terrorism financing.

Given we are a service provider to the industries within scope of the proposed framework, we have limited our responses to the most relevant areas where we can make a meaningful contribution.

Detection of fraud and scam behaviour within digital banking sessions is BioCatch's key area of expertise. Our company works with 30 of the top 100 global banks to detect and prevent fraud and scams. Within Australia, our technology has been deployed across the majority of large banks and helps protect more than 15 million Australians (as at January 2024).

Key Themes of Response

The key themes of our response, that we believe can make the greatest difference in the fight against scams are:

(1) **Reporting, metrics, and benchmarking**. Our belief is that 'what gets measured gets done', so it is critical to ensure that key data points are captured from the businesses covered by the proposed Scam codes. Within the banking sector, it is critical that this data covers both outbound (victim) and inbound (mule) scam related payment activity.

Another element that needs to be captured as part of reporting is general payment volumes so that relative metrics (e.g. value of scam per million $ transactions) may be generated.

Additionally, a benchmarking/leader board style output (ideally public), would be a fantastic tool for increasing transparency and incentivising action. As a fraud manager within a company, if I can use data to show that our business is an outlier compared to peers, then I will have a far greater ability to influence senior leadership to invest in further scam prevention controls. The Payment Systems Regulator's (PSR) APP fraud performance dashboard is a great example of publicly available benchmarking data.

(2) **Making it simpler to share data**. The Framework must enable businesses (including service providers for those businesses) regulated by the Scam code to provide automated signals of high potential scam events (e.g. a payment) between each other.

(3) **Targeted and dynamic in-session intervention** (e.g. education, prompts or questions) and payment holds/delays based on risk signals. These risk signals should incorporate all the following attributes:

a. user profiles (i.e. typical behaviour, demographics, etc)
b. payment attributes (i.e. payee, amount, etc)
c. behavioural biometric and device elements (i.e. digital behaviour such as touch events and mouse movements)
d. recipient account (mule) risk profiles
e. threat intelligence such as historical fraud and scam cases

(4) **Money mules**. Controls mandated by the Framework need to be extended to cover not only outbound (victim) scam events, but also inbound (money mule) activity. The bottleneck for any scam event is exfiltrating the funds, and therefore this step needs to be covered by the Framework. Additionally, many scam types (such as BEC), are extremely difficult to detect if only focusing on risk signals from the sending party, therefore understanding and managing the risk of the destination account (i.e. the mule) is critical to providing a comprehensive solution. Money mule detection must be be prior to criminal funds being received wherever possible. Banks that do not implement effective controls for detecting money mules, are further enabling the growth in scam losses and ultimately money laundering.

Response in relation to bank-specific obligations

Our belief is that the possible bank specific obligations outlined in the Scams Consultation paper make for an excellent list of baseline controls. We've summarised our thoughts as to how they may be refined or extended further to reduce the impact of scams.

Bank Prevention Obligation	BioCatch Response
A bank must implement processes to enable confirmation of the identity of a payee to reduce payments to scam accounts.	Confirmation of payee (COP) is an effective control to help prevent consumers from making scam payments. However, as demonstrated in other markets, it is not a silver bullet and may be bypassed with amended scammer scripts, account takeover new account identity theft, and refund scams.
A bank must implement processes to verify a transaction is legitimate where a consumer undertakes activity that is identified as having a higher risk than their normal activity and is or is likely to be a scam.	We agree with this control but believe the key to the success is not only processes that are implemented to verify transactions, but also the inputs that will accurately determine whether a payment is higher risk. For example, a large payment to a new recipient is a common (legitimate) example and would not be practical for banks to verify all transactions that meet this definition. Instead, we believe the following combination of factors must be used: • **user profiles** (i.e. typical behaviour, demographics, etc) • **payment attributes** (i.e. payee, amount, etc) • **behavioural biometric and device elements** (i.e. digital behaviour such as touch events and mouse movements) • **recipient account (mule) risk profiles** • **threat intelligence** such as historical fraud and scam cases Additionally, we believe that targeted and dynamic in-session intervention (e.g. education, prompts or questions), based on a combination of risk signals above will make for an excellent control to intervene in scams events in real-time.

A bank must have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). Additional steps must be taken if the consumer is identified as having a higher propensity to be affected by a scam.	For this control to be effective, we believe that some specific guidelines around definitions of vulnerable customers will need to be included in the obligations. For example, elderly, new immigrants, and non-native English-speaking customers could be included within the designated vulnerable segment(s).
A bank must implement and have in place processes and methods to detect higher risk transactions and take appropriate action to warn the consumer, block or suspend the transaction, or as well as take other measures to reduce scam activity and limit exit channels for the proceeds of scams, including blocking or disabling the scammer account (if in the same bank) or working with the recipient bank to do so.	As defined above, we believe a combination of the following five elements is key to determining the risk of any given transaction: • **user profiles** (i.e. typical behaviour, demographics, etc) • **payment attributes** (i.e. payee, amount, etc) • **behavioural biometric and device data** (i.e. digital behaviour such as touch events and mouse movements) • **recipient account (mule) risk profiles** • **threat intelligence** such as historical fraud and scam cases An additional control that should be considered is the ability to send a notification to the bank of the intended recipient account (i.e. mule), that a high risk or scam payment was blocked to that specific account. This will enable the receiving bank to review the account and apply appropriate treatment (e.g. close the account) if is confirmed as a mule account.

Bank Detection and Disruption Obligation	BioCatch Response
A bank must have in place methods or processes to identify and share information with other banks that an account or transaction is likely to be or is a scam.	BioCatch is very supportive of this obligation. For the benefit of this obligation to be maximised, we believe that the Framework must support banks to the navigate through any applicable government legislation such as the privacy act. Additionally, the Framework must allow service providers (such as BioCatch) to the banks to share data on the bank's behalf with appropriate authorisation.
A bank must have in place processes to act quickly on information that identifies an account or transaction is likely to be or is a scam, including blocking or disabling the scammer account or the transaction (if in the same bank) or working with the recipient bank to do so.	BioCatch supports this intended obligation.

Bank Response (obligations to consumers)	BioCatch Response
A bank must have user-friendly and accessible methods for consumers to immediately take action where they suspect their accounts are compromised or they have been scammed (e.g. an in-app 'freeze switch').	BioCatch supports this intended obligation.
A bank must assist a consumer to trace and recover transferred funds to the extent that funds are recoverable, including a receiving bank to revert a transfer within 24 hours of receiving a recall request from a sending bank.	BioCatch supports this intended obligation.
A business must respond to an information request from ASIC within the timeframe specified.	BioCatch supports this intended obligation.

Response to List of Stakeholder Questions

Questions on the proposed Framework	BioCatch 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?	Yes. The greatest scam related impacts to consumers currently are within Banking, Telecommunications and Digital Communications industries.
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?	N/A. BioCatch is not well placed to comment on this question.
3. Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?	N/A. BioCatch is not well placed to comment on this question.
4. Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?	N/A. BioCatch is not well placed to comment on this question.
5. Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?	Yes. We believe the core principles are covered and are flexible enough to incorporate other sectors in the future.
6. What future sectors should be designated and brought under the Framework?	Sectors that should be in consideration for coverage of the framework may include: - Payment platform providers (e.g. PayPal) - Superannuation and wealth management - Non-bank lending and credit/debit card providers - FinTech providers - Cryptocurrency exchanges - Gaming and gambling - Share trading and investment platforms - Airlines, hotels and travel providers - Large eCommerce merchants - Online digital services and marketplaces - Government services (e.g. ATO)

7. What impacts should the Government consider in deciding a final structure of the Framework?	The impacts that should be considered could include: - Organisational costs to implement - Net benefit for consumer vs. investment/change required - Scam victim's (consumer or businesses) ability to seek recourse and resolution - Simplicity to administer - Longevity. How easily/quickly criminals could pivot to defeat the proposed control. - Organisational size. Ensuring that the controls mandated by the Framework are proportionate, achievable and fair relative to the company's available resources. - Burden on consumer, private and government entities. - First party fraud. The largest credit card fraud type in the United States is now first party fraud (aka false claims or friendly fraud).

Questions on definitions	BioCatch 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?	From our experience working with banks around the world over the past 10+ years, we believe that it is appropriate to align the definitions as proposed. In summary, fraud are unauthorised transactions by the malicious third party and scams involve authorised transactions for misrepresented goods or services.
9. Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?	Yes. We agree broadly with this definition. The only enhancement we would propose, would be to extend the definition to cover businesses (e.g. victims of BEC scams) and not only individual consumers.
10. Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?	Yes. Financial reasons are key measurable impacts, and others non-measurable impacts (e.g. emotional harm) are typically linked to a financial loss outcome.
11. What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?	As per question 9, the only impact that could be considered in addition to impacts listed, is for scenarios where the victim is a business (e.g. from a BEC scam).
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?	N/A. BioCatch is not well placed to comment on this question.
13. Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?	Industry specific codes, as this will allow for agility and future amendments as the scam landscape evolves.
14. What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?	N/A. BioCatch is not well placed to comment on this question.

Questions on overarching principles-based obligations	BioCatch Response
15. Are there additional overarching obligations the Government should consider for the Framework?	Other overarching obligations that should be considered are in relation to privacy legislation. Specifically: (a) making it easier to share data between organisations for potential scam cases (b) protecting the ability of companies covered by the Framework to collect and store the data necessary to protect their customers from scams. (c) Ensuring that mobile platform providers (e.g. Google and Apple) enable companies covered by the code to collect the data necessary to protect their customers from scams. By Apple and Google restricting access to data under privacy concerns, they are inadvertently restricting access to valuable data that will assist to quickly and effectively detect scams and mules
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?	N/A. BioCatch is not well placed to comment on this question.
17. Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient and safe provision of services to consumers?	N/A. BioCatch is not well placed to comment on this question.
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?	N/A. BioCatch is not well placed to comment on this question.
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?	N/A. BioCatch is not well placed to comment on this question.

Questions on anti-scams strategy obligation	BioCatch Response
20. What additional resources would be required for establishing and maintaining an anti-scam strategy?	The additional resources required to establish and maintain an anti-scam strategy will include: - Operational scam detection and prevention teams - Analytics and data science - Additional call centre staff - Case management and dispute resolution teams - Compliance and legal resources - Customer communications and education resources
21. Are there any other processes or reporting requirements the Government should consider?	Within the banking industry code, the key addition that should be considered for reporting is relating to money mule accounts. Each bank covered by the code should report on both aspects of scam events - the outbound (victim) and inbound (mule) metrics.
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?	- Key (general) pillars of strategy - High level statistics (case numbers, prevented, etc) - Reimbursement rates - Future plans
23. How often should businesses be required to review their anti-scam strategies and should this be legislated?	Based on experience with the rate of change in the fraud and scam landscape, plus the development of AI, we feel that annual review of anti-scam strategy should be the minimum cadence.
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 agree that anti-scam strategy should be signed off by the highest level of governance. This would be like how cyber security strategies are currently managed and governed by businesses.
25. What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?	N/A. BioCatch is not well placed to comment on this question.

Questions on information sharing requirements	BioCatch 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?	The key resources required would be support to navigate the relevant privacy legislation to enable data sharing.
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?	Example safeguards that could be implemented to ensure data sharing is completed in a compliant manner are case sampling and regular / random audits.
28. What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?	As mentioned earlier in the response, most of the Australian banks use BioCatch technology and therefore this network would be well placed to achieve some of the data sharing objectives of the Framework.
29. Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?	The three key hurdles for potential data sharing include (1)privacy regulation, (2) technical infrastructure to share relevant signals/intelligence in a timely manner and (3) 'Tipping Off' rules as outlined in the AML/CTF Act 2006. As mentioned earlier in the response, BioCatch could help with part (2) for banks covered by the Framework.

Questions on consumer reports, complaints handling and dispute resolution	BioCatch 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?	One of the key gaps that needs to be considered for the purposes of this Framework is false claims (also known as first party or friendly fraud). One of the unintended consequences of mandatory reimbursement legislation will be criminals making millions via false claims. A clear example is the credit card chargeback dispute frameworks. According to the Merchant Risk Council (MRC), first party misuse represents at least 18% of all reported fraud. The problem has become so great in the eCommerce space, that Visa announced a new global program in September last year to specifically address first party fraud. https://lnkd.in/ga8zEShc Additional information about dispute resolution and frameworks may also be accessed via the link below. https://www.biocatch.com/blog/liability-lessons-digital-banking-scams
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?	N/A. BioCatch is not covered by the EDR schemes.
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?	N/A. BioCatch is not well placed to comment on this question.
33. Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?	N/A. BioCatch is not well placed to comment on this question.

Questions on sector-specific codes	BioCatch Response
34. Are sector-specific obligations, in addition to the overarching obligations in the CCA, appropriate to address the rising issue of scams?	Two key items that would assist are: (1) real-time phone porting data being made available to organisations using SMS OTP for second factor authentication by telecommunication providers. (2) the mobile device platform providers (i.e. Apple and Google) providing access to additional relevant data for businesses covered by the Framework to better protect consumers from scams.
35. Are there additional obligations the Government should consider regarding the individual sector codes?	N/A. BioCatch is not well placed to comment on this question.
36. Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?	N/A. BioCatch is not well placed to comment on this question.
37. Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?	N/A. BioCatch is not well placed to comment on this question.
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?	N/A. BioCatch is not well placed to comment on this question.
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?	N/A. BioCatch is not well placed to comment on this question.
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?	N/A. BioCatch is not well placed to comment on this question.

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?	N/A. BioCatch is not well placed to comment on this question.
42. Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?	N/A. BioCatch is not well placed to comment on this question.

Questions on approach to oversight, enforcement and non-compliance	**BioCatch 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?	N/A. BioCatch is not well placed to comment on this question.
44. Are there other factors the Government should consider to ensure a consistent enforcement approach?	N/A. BioCatch is not well placed to comment on this question.
45. Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?	N/A. BioCatch is not well placed to comment on this question.

Summary

We believe the controls outlined in the above document will help Treasury department and related stakeholders build a best-in-class framework for protecting citizens from scams. The measures outlined will prove to be practical, achievable, and meaningful in helping achieve the vision of a country that us a world leader in the fight against scams.

Any further questions or consultation would be welcomed by our team, and we would be more than happy to assist further.

Contact

Tim Dalgleish
VP, Global Advisory
Melbourne, Australia
tim.dalgleish@biocatch.com

About BioCatch

BioCatch stands at the forefront of digital fraud detection, pioneering behavioural biometric intelligence grounded in advanced cognitive science and machine learning. BioCatch analyses thousands of user interactions to support a digital banking environment where identity, trust and ease coexist.

Today, more than 30 of the world's leading 100 banks and 150 of the largest 500 rely on BioCatch Connect™ to combat fraud, facilitate digital transformation, and grow customer relationships. BioCatch's Client Innovation Board, an industry-led initiative featuring American Express, Barclays, Citi Ventures, HSBC, and National Australia Bank, collaborates to pioneer creative and innovative ways to leverage customer relationships for fraud prevention.

With more than a decade of data analysis, 90 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges.

For more information, please visit www.biocatch.com.