Meta

Meta's Submission on the *Scams – Mandatory Industry Codes Consultation Paper*

31 January 2024

Executive Summary

Meta shares the Australian Government's intent to disrupt and prevent scams, particularly those that target Australians. This is why we have made significant investments to combat scams and have developed a multi-faceted approach to protecting users on our platforms from scams. This includes policies and systems that prohibit or disrupt this type of behaviour across our services, on and off-platform enforcement, tools and features to help people report fraud and better protect themselves, and education campaigns and partnerships with local government and non-governmental stakeholders.

In Australia, we have invested in partnerships with the Australian Small Business and Family Enterprise Ombudsman, IDCARE and Puppy Scam Awareness Australia as part of which we provide a scam reporting channel and collaborate on the delivery of various scam awareness campaigns that have reached millions of Australians. For example, our 2021 campaign reached over 7.7 million users across Australia and our 2023 campaign reached over 1.2 million users across Facebook and Instagram.

Since September 2017, we have provided a direct scam reporting channel to the Australian Competition and Consumer Commission's (**ACCC's**) Scamwatch so they can promptly share complaints from Australian consumers with respect to scams (this is in addition to our in-app reporting tools that consumers can use). We have also worked with Australian law enforcement and the Office of the eSafety Commissioner (**eSafety**) in relation to investigations into scam and fraudulent activities. To give an overview of the nature of reports we have received and action locally:

- From mid-2022 to date, we received 2381 individual assets referred to us through our regulatory escalations channel by eSafety, the National Anti-Scam Centre (**NASC**), the ACCC and the Commonwealth Bank of Australia relating to issues including financial scams, sextortion and child sexual imagery. All of these assets were reviewed and 1600 found to be violating were enforced on.
- From January 1st 2023 to January 18th 2024, we have received 575 Australian law enforcement data requests specifically relating to fraud and scams. The 575 data requests were predominantly made up of scams related to the non-delivery of items (286), and unspecified scams occurring on (78) or off (103) our platforms. Following this is financial and other investment scams (29), business or government impersonation (9) and romance scams (9).[1]
- From January 1st 2023 to January 22nd 2024, we received 663 Australian law enforcement data requests relating to sextortion. According to the reports we received, 522 of those referred to adults and 141 to minors.[2]

To have the biggest and most lasting impact, we target investigations and disruption on persistent and organised threat actors using a range of signals including our own detection and incoming reports from trusted partners. Between January 2023 to January 2024, for example, we have taken action against hundreds of thousands of accounts, targeting several countries including Australia.

[1] Please note that these data requests are submitted in support of law enforcement investigations and do not always relate to offenses that have occurred on our platform. All requests are manually processed and information provided, and where an account under enquiry is identified as violating, it will also be actioned appropriately.
[2] Similarly, these data requests are submitted in support of law enforcement investigations according to our terms of service and applicable law, and do not always relate to offenses that have occurred on our platform. All requests are manually processed and information provided, and where an account under enquiry is identified as violating, it will be actioned appropriately.

With the announcement of the NASC in July 2023, the Australian Government has signalled that it expects industry to do more to combat scams. To respond to that call, we will be launching a suite of new and additional anti-scam measures in 2024. Described in more detail below, at a high level these include:

- New escalation channels for Australian trusted partners,
- New advertiser verification including heightened verification for higher risk areas, and
- New education resources including an anti-scam resource hub and new consumer campaigns with local partners.

These new measures are in addition to our recent work to engage with the NASC both by responding to direct scam complaints and reports about broader scam trends, and engaging in relevant fusion cell working groups.

They are also in addition to our ongoing work to deploy a variety of methods, such as new machine learning techniques to identify content and accounts that violate our policies. Scams are a highly adversarial space and we are constantly evolving our techniques to keep pace with changing abuse archetypes online.

Against this background, we welcome the opportunity to participate in the consultation on the *Scams-Mandatory Industry Codes*. We recognise the goal of the Proposed Scams Code Framework (**Framework**) is to set clear roles and responsibilities for Government, regulators, and the private sector in addressing scams, promote greater cross-industry collaboration and establish benchmarks across industry to address irregularities in enforcement. Cross-industry collaboration is key, because the majority of scams occur via text message (33%), phone (29%) or email (22%), compared with 6% via the internet and 6% via social network and online forums.[3]

However, the Framework as currently envisaged is complex and potentially duplicative. There are two overlapping layers of regulation, each potentially enforced by different regulators and each with potentially different but cumulative penalties. The rationale for such a regime is not clear and it is likely to lead to inconsistencies and compliance challenges for industry. In addition, many of the proposed obligations do not seem to be effective, proportionate or targeted to combat scams.

Given the significant existing and increasing investment by companies such as Meta in combating scams, and given the extensive regulatory reporting and obligations already applicable to digital platforms under other regulatory schemes, it is important that any new obligations are narrowly targeted and evidenced based to achieve the intended effect of incentivising industry to invest appropriately in combating scams. There is a risk that some proposed obligations, for example, the proposed eco-system wide obligation to have an anti-scam strategy and undertake the internal processes to prepare, secure high-level sign off and regular review of a strategy against risk assessments and ongoing compliance, is time and effort that could be spent on innovating to detect, disrupt and deter scams. With the highly adversarial and rapidly evolving nature of scams, this obligation potentially requires companies like Meta to be constantly adapting an anti-scam strategy.

By way of further example, given the cross-platform nature of scams, an obligation (as is proposed within as a principal obligation) to prevent further losses to a consumer who has been affected by a scam may be

[3] ACCC, 'Targeting scams: Report of the ACCC on scams activity 2022', April 2023, https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

impossible for digital platforms to achieve. What we have seen is that our and industry's efforts to combat scams are forcing threat actors to rapidly evolve their tactics in attempts to evade detection and enable persistence. One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. This means it can be challenging for one provider to have sufficient information to take action as envisaged under the principles.

There are also some key aspects of the Framework that are the subject of further review and consultation, such as the internal and external dispute resolution measures (respectively **IDR** and **EDR**). These have been the subject of ACCC reports dating back to 2019, but have not yet ripened into detailed proposals at this stage, making it challenging to engage with as part of this consultation. Meta supports dispute resolution processes to ensure that consumers can have complaints and concerns promptly addressed and currently provides a range of these mechanisms for reporting scammer and scam content, and regaining control of hacked accounts.[4] However, it is important to carefully review the details of how to implement any regulatory proposals for specific IDR or EDR mechanisms given the existing appeals channels provided by Meta and the Oversight Board, and also the wide range of existing complaint channels that exist for Australian consumers and businesses. The Framework seems to suggest that the failure to comply with any IDR and EDR process would likely attract significant penalties and other claims, in addition to those for breaches of the principal and sector-specific obligations, making it challenging to comment on the merits of these aspects of the Framework at this stage. Significant work would also be required to build a compliance system, but it is difficult to comment further absent details of the precise mechanics of such a process. It is preferable for these discussions to commence with precise delineation of the focus areas.

Given the Australian Government's recent – and highly commendable – establishment of the NASC and the creation of new initiatives from the broader industry (not only Meta's outlined in this submission but also those recently announced by the banking industry[5]) in response to the fusion cell work under NASC, we respectfully suggest that time be given to allow all of these measures to take effect and the impact of these reviewed, with these data points being fed into an industry-led code to be overseen by the Australian Communications and Media Authority (**ACMA**). We believe that an industry-developed code, registered and enforced by the ACMA will be effective in reducing scam activity whilst applying the minimum necessary regulatory burden across the digital sector, consistent with the stated objectives of the codes in the Consultation Paper. DIGI, with its experience in code development, would be well situated to lead this process on behalf of the digital industry.

This would be consistent with the approach being adopted in the UK, which last year introduced the UK Online Fraud Charter, a voluntary code with extensive industry consultation.[6] This allows for industry to adjust, take learnings from implementation and work together, before a co-regulation or formal law is

---

[4] For example, Facebook, 'Report something', Help Centre, https://www.facebook.com/help/263149623790594; Instagram, 'How do I report a post or profile on Instagram?', https://help.instagram.com/192435014247952/?helpref=uf_share; Meta, 'My account was hacked or someone is using it without my permission', Policies, https://www.meta.com/en-gb/help/policies/safety/hacked-account

[5] In November 2023, the banking industry announced the launch of the Banks have announced the industry-wide Scam- Safe Accord, which will be rolled out over 2024 and 2025: Australian Banking Association, 'Banks unite to declare war on scammers', https://www.ausbanking.org.au/new-scam-safe-accord. which details how much they expend on scam detection, and significant changes to implement Pay ID. These have been demanded for some time by the ACCC (https://www.smh.com.au/business/consumer-affairs/people-are-losing-a-fortune-accc-urges-banks-to-act-as-scam-losses-surge-20220704-p5ayvy.html) but won't roll out until 2024/5 (already in place in EU and UK for some time)

[6] UK Government, *Online Fraud Charter*, 30 November 2023, https://www.gov.uk/government/publications/online-fraud-charter-2023

introduced. Meta, alongside other technology companies, signed the UK Online Fraud Charter to demonstrate our commitment to work together across industry, and with the UK government, to protect the public from online scams.

The reason why it is important to get the incentives and measures by industry to combat scams right is – not just because it is imperative that these are effective and resilient obligations to reduce scams targeting Australia – but also so that any anti-scam measures do not add undue friction to Australian consumers and businesses. Meta provides services to millions of Australian households each day to enable them to connect with friends and family, engage with local communities, and follow a local business, creator or other public figure. Digital services have also democratised commerce, allowing thousands of business owners to easily start a business using the free tools provided by Meta's family of apps. According to research conducted in 2023 by global research firm, ThoughtLab, digital technologies allowed small and medium-sized enterprises (SMEs) in Australia to generate an estimated $306 billion in additional revenue over the previous year.[7] At least three-quarters of the Australian SMEs surveyed for the research reported that Meta's platforms help people to learn about their business, build customer relationships and to market and sell their products and services.[8] In a further global study of small businesses undertaken by Deloitte in 2021, 63% of surveyed SMEs reported that personalised advertising was important in achieving a high return on market expenditure when compared with other marketing tools, while 71% of Australian SMEs using targeted advertising reported that it is important for the success of their business.[9] Given this, it is important that the Framework incentivises narrowly targeted interventions to reduce scams and not add unnecessary friction to small businesses owners competing online for customers with small businesses in other countries.

We look forward to continuing to work closely with the NASC, the Australian Government and across the digital and broader industry on scam reduction.

[7] ThoughtLab, 'The Digital Journey of SMEs in Australia - How small and medium-sized enterprises drive business and economic results through digital innovation', May 2023, https://thoughtlabgroup.com/the-digital-journey-of-smes-in-australia
[8] ThoughtLab, 'The Digital Journey of SMEs in Australia - How small and medium-sized enterprises drive business and economic results through digital innovation', May 2023, https://thoughtlabgroup.com/the-digital-journey-of-smes-in-australia
[9] Deloitte, 'Dynamic Markets - Unlocking small business innovation and growth through the rise of the personalized economy', May 2021, https://scontent-syd2-1.xx.fbcdn.net/v/t39.8562-6/10000000_4303078769743544_7237603050373993547_n.pdf?_nc_cat=109&ccb=1-7&_nc_sid=e280be&_nc_ohc=pC0ob_iecM0AX8dWd9Z&_nc_ht=scontent-syd2-1.xx&oh=00_AfDpwnF68UIyWxrD-1uAwRmt2iM4x-t-xfCuVxPguxA_OQ&oe=65B40E49

Table of Contents

- Executive Summary
- Meta's existing work to combat scams
  - Policies
  - Detection and enforcement against scams
    - On-platform enforcement
      - Ads Review System
      - Removing Fake Accounts
      - Authentication
      - Persistent Violators
    - Off-Platform Enforcement
      - Working with law enforcement
      - Cross-border partnerships
      - Litigation
  - User Tools and Controls
    - Report
    - Ratings and Reviews
    - Ad Library
    - Features to prevent unwanted contact and educate users
  - Awareness campaigns & partnerships
- New anti-scam initiatives
- General comments on the Proposed Scams Code Framework
  - Framework should be fit-for-purpose & evidence based
  - Clarifying the proposed definition of a 'scam'
  - Proposed obligations risk being inflexible and potentially duplicative
  - Concurrent regulator approach with overlapping obligations may cause conflict and confusion
  - Ensuring penalties are proportionate
  - Clarity needed on dispute resolution
  - The importance of effective reporting obligations
  - Complexities and dynamics of the digital space
- Table of Responses to Stakeholder Specific Questions

Meta's existing work to combat scams

Before turning to our comments on the Proposed Framework, we wanted to first share details about our existing investments to combat scams, and also the new initiatives we are undertaking in response to the Australian Government's call for industry, particularly digital platforms, to do more to combat scams targeting Australians. These details provide context to our comments on the Framework.

Combatting scams requires a multi-faceted, whole-of-ecosystem approach. For this reason, we adopt a four-pronged approach: (1) policies that prohibit scams and related behaviour; (2) enforcement both on and off-platform; (3) tools to allow people to block and report scams, but also warn people about potentially suspicious activity; and (4) consumer education initiatives and partnerships.

Policies

Across our services, we have policies that outline what people can and cannot do on our services via our social media features, on our advertising products and on commercial surfaces such as Facebook Marketplace.

For example:

- across Facebook and Instagram, we have a specific Fraud and Deception policy to protect people and businesses on our platform.[10] Under our Fraud and Deception policy, we remove content that purposefully deceives, willfully misrepresents or otherwise defrauds or exploits others for money or property. This includes content that seeks to coordinate or promote these activities using our services,
- our Advertising Standards strictly prohibit deception and misleading behavior,[11] and
- our Commerce Policies prohibit listings with misleading offers.[12]

On WhatsApp, we also have policies and systems that work to detect and enforce against abusive accounts, such as frauds and scams.[13]

In addition, we block the use of specific search terms related to scams, fake reviews, and known bait words. We also have measures in place to make Groups/Pages on Facebook that previously violated our policies less prominent in Feed and in recommendations. This is in line with our Content Distribution Guidelines, where we provide details about the problematic or low quality content that we reduce for distribution.[14] This includes content that contains clickbait links, engagement bait, links to websites that

[10] Meta, 'Fraud and Deception - Policy details', https://transparency.fb.com/policies/community-standards/fraud-deception
[11] Meta, 'Introduction to the Advertising Standards', https://transparency.fb.com/policies/ad-standards
[12] Meta, Commerce policies, 'Prohibited content: Misleading, Violent, or Hateful', https://www.facebook.com/policies_center/commerce/misleading_violent_or_hateful
[13] WhatsApp, *WhatsApp Business Messaging Policy*, https://business.whatsapp.com/policy
[14] Meta, 'Types of Content We Demote', Transparency Centre, https://transparency.fb.com/en-gb/features/approach-to-ranking/types-of-content-we-demote

request unnecessary user data. We also exclude this type of content from being recommended across a range of surfaces, as outlined in our Recommendation Guidelines.[15]

Detection and enforcement against scams

We undertake action to prevent scams both on-platform and off-platform.

On-platform, in order to enforce our policies, we use a combination of artificial intelligence and human reviewers. We have invested significantly in proactive detection technology, by using artificial intelligence and machine learning, to identify and disrupt harmful content and behaviour on our service. Our detection efforts continue to evolve in an effort to identify content that violates our policies, in some cases removing it before anyone sees it. We have around 40,000 people working in safety and security at Meta. Our content review team reviews content 24/7 and we make a point to hire people with the necessary language and cultural context for the markets in which we operate. We also have entire teams dedicated to constantly improving and adapting our systems to proactively identify and block scams.

Every day, we remove millions of violating pieces of content and accounts on Facebook and Instagram. In most cases, this happens automatically with artificial intelligence to detect, restrict, and remove content and accounts that may go against our policies, including our Community Standards, Advertising Standards, and Commerce Policies. Our technology also supports the review teams by prioritising the most critical content to be reviewed, based on severity, virality, and likelihood of a violation. On WhatsApp, we utilise technology that spots accounts engaging in abnormal behavior and we ban over 8 million accounts per month this way, 75% of them without a recent user report.[16]

On-platform enforcement

Ads Review System

In the context of advertisements, our ad review system relies primarily on automated tools to check ads and business assets against our policies. If we detect a violation of our scams policies, we will reject the ad before it is published. Beyond reviewing individual ads, we may also review and investigate advertiser behaviour, such as the number of previous ad rejections and the severity of the type of violation, including attempts to get around our ad review process.[17]

Removing Fake Accounts

Scams are often run by people who manually operate fake accounts. That is why our efforts to detect and stop fake accounts are so crucial. To combat fake accounts, we deploy technology to prevent them from being created and also detect and remove them from the platform. Our detection technology helps us block millions of attempts to create fake accounts every day and detect millions more often within minutes after creation. As outlined in our quarterly Community Standards Enforcement Report, in Q3 2023, for example:

---

[15] Facebook, 'What are recommendations on Facebook?', Help Centre, https://www.facebook.com/help/1257205004624246
[16] WhatsApp, 'About WhatsApp and elections', Help Centre, https://faq.whatsapp.com/518562649771533?helpref=search&query=8&search_session_id=aa13c1b8adbc16c4fa1000313a064321&sr=5
[17] See Meta, 'About advertising restrictions', Meta Business Help Centre, https://www.facebook.com/business/help/975570072950669?id=434838534925385

- We actioned 827 million fake accounts on Facebook, 99.1% of which we detected proactively ourselves via artificial intelligence before a user reported it to us.[18] This is in addition to the millions of fake accounts that we block at the point of creation every day.
- We actioned 413 million pieces of spam content on Facebook, 98.2% of which we detected proactively ourselves via artificial intelligence.[19]

Authentication

If we determine that an account is likely associated with scam behaviour, the account owner must complete a few actions to demonstrate that they are not operating a fake account or misrepresenting themselves. Until they do this, the account cannot be used to reach others. If the owner fails these checks, or if our reviewers determine that there is a violation of our policies, the account will be removed.

Our abuse-fighting team builds and constantly updates a combination of automated and manual systems that help us catch suspicious and/or inauthentic activity at various points of interaction on the site, including registration, friending and following, liking and messaging.

We also require many businesses to undergo verification to confirm the identities of the business and its representatives before they can use certain tools or features. Verification requirements include activities such as:

- Confirmed Page Owner: verifies the authenticity of people or organisations who manage Pages with a large audience.[20]
- Business verification: required for business app developers who want to use certain APIs.[21]
- Authorisation process: verifies the identity and location of advertisers who run ads about social issues, elections or politics,[22] which are also required to include a "Paid for by" disclaimer.[23]

For these processes, we offer business verification, which involves users/advertisers verifying their business with a third party company and/or providing documentation to prove legitimacy.

Persistent Violators

In order to maintain a safe environment for users, we remove accounts or entities that are harmful to the community. We apply penalties that are designed to be proportionate to the severity of the violation and the risk of harm posed to the community. Continued violations, despite repeated warnings and restrictions, can lead to an account being disabled. We have built a combination of automated and manual systems to block and remove accounts that are used to persistently or egregiously abuse our Community Standards. We also disable accounts or entities that have been created or repurposed to evade our enforcement.

---

[18] Meta, 'Community Standards Enforcement Report Q3 2023', https://transparency.fb.com/reports/community-standards-enforcement/fake-accounts/facebook
[19] Meta, 'Community Standards Enforcement Report Q3 2023', https://transparency.fb.com/reports/community-standards-enforcement/spam/facebook/#content-actioned
[20] Facebook, 'About Page transparency', Help Centre, https://www.facebook.com/help/323314944866264
[21] Meta, 'About business verification', Meta Business Help Centre, https://www.facebook.com/business/help/1095661473946872?id=180505742745347
[22] Meta, 'Get authorized to run ads about social issues, elections or politics', Meta Business Help Centre, https://www.facebook.com/business/help/208949576550051?id=288762101909005
[23] Meta, 'Create disclaimers and link ad accounts', Meta Business Help Centre, https://www.facebook.com/business/help/488070228549681?id=288762101909005

Off-Platform Enforcement

Off-platform, we work with our legal teams, local authorities and civil society partners to consider and take appropriate action against bad actors.

Working with law enforcement

We respond to valid legal requests by law enforcement and regulators as they try to identify and pursue individuals and organisations committing these crimes. We share information with law enforcement and regulators in cases where it might be necessary to prevent scams or other types of illegal activity, in line with our terms of service[24] and applicable law.

Cross-border partnerships

Bad actors create an adversarial environment and continuously evolve their tactics - usually operating across multiple countries, moving from one platform to another, or offline where digital platforms have no visibility. Thus, we work with international law enforcement agencies across the countries in which we operate to tackle cross-border scammers and to hold them accountable. This includes working with INTERPOL.

Litigation

As part of Meta's ongoing efforts to enforce our Terms and protect people against abuse, we have brought legal action against individuals and entities responsible for using our platforms to scam people. For example:

- In 2019, we filed suit in California against a company called ILikeAd Media International Company Ltd. and two individuals for violating our Terms and Advertising Policies.[25]
- In 2021, we filed a case against four individuals residing in Vietnam, who used a technique known as "session theft" or "cookie theft" to compromise accounts of employees of advertising and marketing agencies and then ran unauthorised ads.[26]
- In 2022, Meta and a financial services company filed a joint lawsuit, the first of its kind, against two Nigerian-based individuals who engaged in phishing attacks to deceive people online and gain access to their online financial accounts. We had taken several prior enforcement actions against the defendants, including disabling Facebook and Instagram accounts, blocking impersonating domains on its services and sending a cease and desist letter. This joint lawsuit represented a major step forward in cross-industry collaboration against online impersonation.[27]
- In 2022, we filed a lawsuit against an Australian resident, Chad Taylor Cowan, for providing a fake engagement service directed at Facebook. Cowan operated a website that provided fake reviews and feedback to businesses in order to artificially increase their Customer Feedback Score.[28]

---

[24] See Meta's Privacy Policy at<https://www.facebook.com/privacy/policy/>
[25] Meta, 'Taking Action Against Ad Fraud', Newsroom, 5 December 2019, https://about.fb.com/news/2019/12/taking-action-against-ad-fraud
[26] Meta, 'Combating E-Commerce Scams and Account Takeover Attacks', Newsroom, 29 June 2021, https://about.fb.com/news/2021/06/combating-e-commerce-scams-and-account-takeover-attacks
[27] Meta, 'Taking Legal Action Against Financial Services Scams', Newsroom, 8 February 2022, https://about.fb.com/news/2022/02/taking-legal-action-against-financial-services-scams
[28] Meta, 'Taking Action Against Fake Customer Feedback and Reviews', Newsroom, 16 March 2022, https://about.fb.com/news/2022/03/taking-action-against-fake-customer-feedback-and-reviews/

User Tools and Controls

Combating scams requires a whole-of-ecosystem approach, which is why we also provide easy access to user reporting and other tools to help people have a safer experience on our services and to have more information about the accounts with which they interact.

Report

Every single thing on Facebook and Instagram can be reported – page, profile, post, photo, comment, message - and we have dedicated reporting options for scams. On WhatsApp and Messenger, we encourage users to report suspected scam conversations or contacts directly within the app, which provides us with a limited number of unencrypted messages from the user's device for review, which we take action against if violating.[29]

In addition, we have different reporting channels for different groups - for example advertisers, brand rights holders, governments and law enforcement agencies. Reporting sends a signal to us that something is wrong, and helps improve the quality of users' experience on our apps.

Ratings and Reviews

Likewise, our ratings and review features in Facebook Pages,[30] Facebook Marketplace,[31] and Instagram Shops[32] are designed for users to provide feedback to other users. These features give other users more context about the business or individuals they are interacting with, so they can decide for themselves who to trust.

Ad Library

When it comes to ads, we have a publicly available Ad Library[33] that enables people to search for all active ads across Facebook and see when the ad was posted, which platforms they have been posted on and who is sponsoring the ad.

Features to prevent unwanted contact and educate users

We have implemented a number of privacy and safety features to protect users on our services, including when they are contacted by someone they are not connected to.

These include:

- ***Message request limits on Instagram:*** We use machine learning models as described above to identify accounts with unusual behavioural patterns that correlate with scams. When such accounts are identified, we limit the number of message requests they can send per day based on

[29] WhatsApp, 'How to block and report contacts', Help Centre, https://faq.whatsapp.com/1142481766359885/?helpref=search&cms_platform=android; Messenger, 'How do I report an end-to end encrypted chat in Messenger?', Help Centre, https://www.facebook.com/help/messenger-app/498828660322839/?cms_platform=iphone-app&help
[30] Facebook, 'How Page ratings are determined', https://www.facebook.com/help/500762053364226?cms_platform=www&helpref=platform_switcher
[31] Facebook, 'How ratings work on Facebook Marketplace', https://www.facebook.com/help/915385548593204/?helpref=related_articles
[32] Instagram, 'Review an item you purchased on Instagram', https://help.instagram.com/209709211058981
[33] Meta, *Ad Library*, https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=IE&media_type=all

risk to reduce their reach.

- ***Safer Message Requests on Instagram*:** Before being able to message with an unconnected user on Instagram, people must send an invite to get permission to connect.[34] These message request invites from a sender are limited to one text message only, so people cannot send any photos, videos, or voice messages, or make calls, until the recipient has accepted the invite to chat.
- **Safety Notices on Messenger and Instagram:** Too often, people interact with someone online they think they know or trust, when it is really a scammer or imposter. Messenger already filters some potential spam or malware and offers tips to avoid common scams. Our safety notices also help educate people on ways to spot scams or imposters and help them take action to prevent a costly interaction. We also have recently introduced similar contextual scam prevention safety notices in Instagram Direct.
- **Information about people sending messages:** In Messenger and Instagram, we provide the recipient of the contact with additional information about the account. This includes information such as relationship (i.e. mutual follows, friends in common, etc.) and age of account to help people identify potentially inauthentic accounts that were recently created. For Instagram, we also include account activity (i.e. number of posts).
- **Educating users on avoiding scams:** On Messenger, we provide safety tips to educate people on spotting suspicious activity and taking action to block, report or ignore someone when something does not seem right. We developed these safety tips with machine learning that looks at someone's activity on our apps to help educate people on avoiding scams or spotting impersonations.[35] More broadly, we publish tips on avoiding scams across our services.[36]

Likewise, when a user receives a message on WhatsApp from someone who is not in their contact list, they immediately receive a prompt asking if they want to block or report them,[37] and if a user is added to a group from someone outside their contact list, WhatsApp provides an option for them to "report" or "exit" the group. We also empower users to silence calls from unknown callers (people you haven't previously contacted or saved as a contact) through the privacy settings, to prevent unwanted contact[38]. In addition, users can choose who can add them to a group, among "everyone" (that includes people outside the user's address book), "my contacts" (people included in user's address book) or "my contacts except.." (to exclude particular people who are included in the address book).[39]

Awareness campaigns & partnerships

Tackling scams is an industry wide challenge, and we have partnered with several organisations in Australia to educate users and businesses on our platforms on how to stay safe online. In particular, we have worked with IDCare, Puppy Scam Awareness Australia and the Australian Small Business and Family Enterprise Ombudsman to deliver a scams awareness campaign in late 2021, including tips on how to identify different types of scams and report them, and account safety and cybersecurity tips. The

---

[34] Meta, 'Giving Teens and Parents More Ways to Manage Their Time on Our **Apps', Newsroom, 27 June 2023,** https://about.fb.com/news/2023/06/parental-supervision-and-teen-time-management-on-metas-apps

[35] Messenger, 'Stay in Control with Messenger Safety Features', 9 February 2021, https://messengernews.fb.com/2021/02/09/stay-in-control-with-messenger-safety-features

[36] See, for example, Meta, 'How to avoid scams and phishing attempts', https://www.meta.com/en-gb/help/policies/safety/avoid-scammers; Facebook, 'Avoiding scams on Facebook', Help Centre, https://www.facebook.com/help/1674717642789671

[37] WhatsApp, 'How to stay safe on WhatsApp', Help Centre, https://faq.whatsapp.com/1313491802751163?helpref=faq_content

[38] How to silence unknown callers https://faq.whatsapp.com/1238612517047244?helpref=faq_content

[39] How to change group privacy settings https://faq.whatsapp.com/1131457590844955/?cms_platform=android

campaign reached over 7.7 million people in Australia. We also worked with Australian creators to launch a new scam education campaign to coincide with 2023 national Scams Awareness Week, in partnership with local creator @joshandmattdesigns .

In late 2022, we updated our Meta Boost digital skills training curriculum for small businesses to include a new module on online safety and cybersecurity, which shared tips and advice for SMEs on how to protect their accounts and Pages from scams and fraudulent activity. We delivered this module as part of our Meta Boost training events in Byron Bay and Western Sydney in 2022 and 2023, in partnership with the Byron Bay, Mullumbimby and Majors Bay Chambers of Commerce.[40]

In May 2020, we introduced safety notices in local languages on Messenger that pop up in a chat and provide tips to help people spot suspicious activity and take action to block or ignore someone when something doesn't seem right.[41] These safety notices also help educate people on ways to spot scams or imposters and help them take action to prevent a costly interaction.

In all of our education efforts, we encourage people to use our in-app reporting tools when they see any suspicious activity, such as a suspected Facebook Marketplace scam.[42] Our centralised Help Centre also provides people with tips on how to avoid scams on Facebook, including reporting suspected scams[43] and protecting themselves from phishing.[44]

Scams are a highly adversarial space and we are constantly evolving our techniques to keep pace with changing behavior online. We currently use (and continue to explore) a variety of methods such as new machine learning techniques to identify content and accounts that violate our policies, as well as working with government, NGOs, and law enforcement agencies to understand new techniques that scammers deploy to circumvent our system.

We have had a dedicated channel for ACCC to report scams content to us since September 2017. We review the content that is reported and take appropriate action if it is found to be violating.

Since its establishment last July 2023, we have actively engaged with the various processes established by the NASC and working towards increased industry collaboration to identify what more all of industry can be doing to combat scams. Beyond removing individual scam reports, we are working closely with the NASC to also identify scams trends and address these. Cross-industry collaboration is key, because the majority of scams occur via text message (33%), phone (29%) or email (22%) compared with 6% via the internet and 6% via social network and online forums.[45] This is why we will continue to invest in this area and work with others to find collaborative solutions to stop scams.

---

[40] See Meta Policy AU, 'Meta heads to Byron Bay to boost small businesses', Medium, 1 February 2023, https://medium.com/meta-australia-policy-blog/meta-heads-to-byron-bay-to-boost-small-businesses-da79e6a9574e; Meta Policy AU, 'Meta heads to Western Sydney to boost small businesses', Medium, 22 May 2023, https://medium.com/meta-australia-policy-blog/meta-heads-to-western-sydney-to-boost-small-businesses-4a2233d570c8

[41] Messenger, 'Preventing Unwanted Contacts and Scams in Messenger', 21 May 2020, https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger

[42] Facebook, 'Report a Facebook Marketplace scam', Help Centre, https://www.facebook.com/help/1295340050874305?cms_platform=www&helpref=platform_switcher

[43] Facebook, 'Avoiding scams on Facebook', Help Centre, https://www.facebook.com/help/1674717642789671/?helpref=uf_share

[44] Facebook, 'Protect yourself from phishing on Facebook', Help Centre, https://www.facebook.com/help/phishing

[45] ACCC, 'Targeting scams: Report of the ACCC on scams activity 2022', April 2023, https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

New anti-scam initiatives

We recognise that the Australian Government expects industry to do more to combat scams, especially those targeting Australians.

Combating scams is an ongoing challenge across many industries. We have seen that the efforts of Meta and others within industry to combat scams, are forcing threat actors to rapidly evolve their tactics in attempts to evade detection and enable persistence. One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. When bad actors count on us to work in silos while they target people far and wide across the internet, we need to work together as an industry to protect people. This is why the work of the NASC in bringing industry together to encourage greater cross-industry collaboration is helpful. It is also why a number of our new anti-scam measures include faster ways for us to receive reports of problematic content or accounts that our existing investments may not identify initially.

In order to improve our detection, we make changes to our machine learning models by ingesting new scam trends and signals that we receive from users' reports and government escalations. We are also building a system for evaluating and ensuring the precision of our machine learning. Over time, these changes allow us to improve our proactive detection and enforcement at scale. We are also currently exploring the development of tools by introducing new technology that would allow our system to detect better, faster and receptive to the newer scams trends.

To respond to the Government's call for industry to do more to combat scams targeting Australians, we are undertaking a suite of new measures:

- **New cross-industry escalation channels for Australian trusted partners**:
    - *The Fraud Intelligence Reciprocal Exchange Channel (FIRE)* – is a direct channel for trusted partners to report online fraud intelligence to Meta. To support streamlining reports from the banking industry in early 2024, we will pilot a new dedicated channel for selected banks to fast track suspected scams on Facebook and Instagram directly to the relevant Meta teams. Information shared by this channel will help both parties to better reduce the harm generated by the ever-changing online scam landscape.
    - *New WhatsApp Trusted Partner Reporting Channel* – we are developing a new WhatsApp Trusted Partner Reporting Channel for NASC to help streamline the reporting process. This will be launched by mid-2024.
- **New advertiser verification:** we are progressing plans to test lightweight verification for all advertisers with heightened measures for higher risk areas, specifically:
    - *Financial Service Ads Verification* – we recognise the strong focus of the Australian Government on investment and financial services scams. A key element of our multi-pronged strategy in tackling misleading ads is to introduce greater transparency around the people or organisations advertising on our platforms so that people may scrutinise and hold these advertisers accountable. We have seen the effectiveness of such an approach with the political ads transparency tools we have deployed since 2018. This enabled regulators, journalists, watchdog groups, researchers, academics and people in general to scrutinise social issues, elections and political ads in the advertising ecosystem, as well as report ads that they believe are in violation of our advertising policies. We are

exploring ways to do the same for financial services ads and looking to launch ads verification and transparency measures for such ads in the second half of 2024, which will include:

- Identity Verification: Advertisers who run financial ads will have to undergo either business verification (in the event the advertiser can do so for their business), or if that's not possible, ID verification for the person paying for the ad which contains a country-location check.
- Disclaimer: Financial services ads will carry a disclaimer that identify them as financial services ads and include links to more information about the advertiser.
- Ad Library: All active financial ads will be publicly displayed in the Ad Library. People can scrutinize the ads running on Facebook and Instagram in the Ad Library and report ads that are missing the financial ad disclaimer.

- *Higher levels of verification for new ad accounts* - we will also be testing increased levels of verification for all new advertisers later this year. Our analysis indicates that the vast majority of ad scams detected originate from accounts that are less than 90 days old. We will therefore focus our efforts on applying a higher level of verification to new ad accounts and test verification for new advertisers. In measuring the impact of this test, we will be looking at a number of factors, including the impact on the advertiser completion rates and harm reduction advertiser completion rates and the impact to harm reduction. If this test is successful, we expect to be able to roll this out to all new advertisers targeting Australia later this year.

- **New education resources and awareness campaigns including a launching a new Anti-Scams Resource Hub and new consumer campaigns with local partners**
  - *Developing a new anti-scams resource hub* - to expand our efforts to educate users and businesses on how to identify and avoid scams we are launching a new anti-scams resource hub in the first half of 2024. This hub will include information about the latest trends in scams, Meta's latest advances in cybersecurity, tips and educational material, and quick links for reporting scams, account access issues, and IP, brand rights protection and impersonation issues.
  - *New local scam awareness campaigns* – leveraging the new resource hub and our existing partnerships, we will launch new scam awareness and consumer campaigns in 2024, including new education materials addressing scam prevention on WhatsApp and cybersecurity for small businesses.

General comments on the Proposed Scams Code Framework

Framework should be fit-for-purpose & evidence based

We support the intent of the Framework – to set clear roles and responsibilities for the Government, regulators, and the private sector in combating scams. With respect to the private sector, this includes ensuring that measures are in place to prevent, deter, detect and disrupt, and respond to scams.

At Meta, we have acted on the Australian Government's call for industry to step up and do more, including through cross-industry collaboration, to combat scams targeting Australians. This is why we have announced a suite of new anti-scam initiatives (outlined above). For some of these initiatives – such as verification of certain advertisers – we are testing these measures and their efficacy, before committing to these definitive measures.

We note that other industries such as the banking industry have recently also announced new initiatives that will roll out over 2024 and 2025.[46] Given the evolving and adversarial nature of scams, it is important to allow new initiatives by industry time to take effect and review their potential impact.

The Consultation Paper also recognises that the NASC is building its data-sharing capability to enhance scams information sharing across the ecosystem which will result in improved quality, timeliness and coverage over the next three years.[47]

Given the recency of both industry and the Government's increased anti-scam measures, it is not yet possible to design a full regulatory framework with the evidence from these early-stage initiatives. It is also not yet clear where more is needed nor the precise roles and responsibilities for each stakeholder within the ecosystem. For example, we are continuing to work with the NASC on how we can better streamline the scam reporting process to help us with actionable data. Consequently, the Framework risks being premature and diverting investment away from detecting and enforcing on scam activity, and incentivising industry to prioritise regulatory compliance over further innovation to disrupt and deter scams.

Given the NASC was only established in July 2023 and the cross-industry collaboration has only been in place for several months, together with additional initiatives being undertaken by industry stakeholders including Meta, we suggest that further time be taken to review and consider the data and evidence on the efficacy of these new initiatives to inform the Framework of what works to more effectively combat scams.

At present, it is not clear what evidence underlies many of the proposed ecosystem-wide obligations in the CCA, for example, and how these will be effective in reducing the number of scams targeting Australians. For example, the internal process to prepare, secure high level sign off and regular review of a strategy against risk assessments and ongoing compliance is time and effort that could be spent on

[46] In November 2023, the Australian banking industry announced the launch of the Scam-Safe Accord, comprising a comprehensive set of industry-wide anti-scam measures to disrupt, detect and respond to scams. These include an industry-wide confirmation of payee solution to customers, with name checking technology so customers know who they are dealing with. These significant measures will be built and rolled out over 2024 and 2025: Australian Banking Association, 'Banks unite to declare war on scammers', https://www.ausbanking.org.au/new-scam-safe-accord

[47] The Treasury, *Scams - Mandatory Industry Codes Consultation Paper*, November 2023, p14, https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf

innovating to detect, disrupt and deter scams. These provisions seem specifically intended to incentivise companies to prioritise regulatory compliance over promoting a safer and more secure ecosystem. Similarly, it is not clear how the Framework will apply to other sectors that play a key role in the creation and commission of scams, such as dating sites, crypto-currency exchanges, superannuation funds, and payment service providers. For example, in 2022, the ACCC reported that the most common payment method for investment scams was cryptocurrency.[48] The absence of a holistic view of the scams ecosystem means a piecemeal approach that could undermine the Framework's overall effectiveness, and potentially lead to unintended consequences, both for markets and scam behaviour.

Ideally the regime should be designed with the benefit of a clear assessment of (a) existing industry efforts to target and prevent scams, (b) industry best practice in this area, especially where scams are conducted online and across different platforms, (c) the best form of cross-industry and industry-government collaborations, and (d) any gaps or deficiencies in the NASC capabilities.

Allowing the NASC to develop its capabilities and share the lessons learned with the Government and digital communications providers, and for digital communications providers to report back on the progress on initiatives will allow for the design and implementation of an evidence-based, effective, proportionate and practical regulatory regime. It would also be in line with the approach taken in the UK, where the first step toward industry cohesion was the development of industry commitments in the UK Online Fraud Charter. The UK Online Fraud Charter encourages innovation, cross-industry information sharing and places the regulator in the best position to develop an evidence-based regulatory framework in the future.

Finally, when considering the structure and obligations of the Framework, particularly any sector-specific code for digital platforms, it is important to understand the complex and highly dynamic nature of the digital space and the ways in which scammers quickly adjust their tactics to evade detection. Given this adversarial environment, any regulatory framework should contain sufficient flexibility to allow tactics and responses to scams to quickly adjust and adapt.

Clarifying the proposed definition of a 'scam'

We understand the intent of capturing a broad range of behaviour that leads to harm to consumers, but caution against a definition where there are overlapping concepts, for example, criminal or privacy law, which could create confusion and undermine the effective implementation of obligations under the framework. In this context, we consider the proposed definition of 'scam' as *'a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means'* to be overly broad. Specifically, we suggest removing 'personal information' from the proposed definition to avoid conflating the issue of scams with issues relating to privacy and data breaches, and the risk of setting unclear and confusing obligations that are unable to be effectively implemented. We are also unclear how 'designed to' will be applied in practice, noting that any definition should focus on both a clear and verifiable intent element as well as actual impact to victims.

This approach would align with Meta's policies relating to fraud and deception, which focus on content and behaviours that purposefully intend to deceive, willfully misrepresent or otherwise exploit others for money or property, including content that seeks to coordinate or promote such activities using our

[48] ACCC, Targeting scams: Report of the ACCC on scams activity 2022, April 2023, https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

services. This approach also aligns with the UK Fraud Charter, which focuses solely on financially motivated fraud and deception.

Proposed obligations risk being inflexible and potentially duplicative

We recognise the policy intent of introducing a new overarching regime under the CCA together with sector specific legislation to enable Government or regulators to develop codes and standards for designated sectors.

Whilst this arrangement seems intended to set out the key objectives of the regime and provide the necessary powers to establish and enforce the mechanics of the regime (with those mechanics set out in a code of conduct), the current proposal would go much further and establish in primary legislation a detailed set of 'principles-based obligations'. It would in effect create a code of conduct within the CCA. This seems duplicative and unnecessary from a regulatory perspective. It would also cut across one of the Treasury's stated objectives that the Framework should be 'flexible and responsible to future changes in the scams ecosystem'.

Rather than having a single set of high level obligations applicable to all industries as a code under the CCA, with potential overlap in the areas within scope of the sector-specific codes, we suggest that further work should be conducted with industry representatives to develop sector-specific sets of requirements, with the benefit of industry expertise and co-regulatory design. At present, the obligations in the primary law and a digital-sector specific code cover the same areas and risk being duplicative and confusing as industry is working to build compliance systems. For example, there is an obligation in the primary law for a business to detect, block and prevent scams from initiating contact with consumers. There is a similar obligation in the digital communication platform specific obligations for a provider to detect high risk interactions and take appropriate action to block the interaction. Both of these obligations seem to be targeted at the same issue (i.e. blocking interactions with scammers). It will be difficult for industry to build for compliance if they are faced with overlapping, but slightly different, obligations, potentially enforced by different regulators.

We also suggest that a balanced approach be taken in assessing compliance with the Framework's obligations and recommend prioritisation of scams that pose the greatest risk of harm to consumers. This approach will ensure that the most pernicious scams are being addressed and avoid the risk of unintended adverse consequences. Taking user reports as an example, not all reports are equal in terms of the level of risk and harm that they may cause. Some reports may be benign, where there is no immediate harm or there are no or only a small number of views, while other posts may be spreading rapidly and pose a greater harm to individuals. Requiring digital platforms to treat all reports equally risks unintended, adverse consequences, such as:

- Forcing companies to be less diligent with the review processes in order to meet fixed timeframes, which may lead to over-enforcement and the stifling of free expression.
- Forcing companies to treat all user reports equally, rather than prioritising reports that may pose a greater harm to an individual, or multiple individuals.

It is important to balance expediency with the risk of harm and rights of users. Furthermore, if a timeframe should be specified, we recommend that flexibility is included to allow for what is reasonable, having regard to the context and complexity of the content being reported.

Concurrent regulator approach with overlapping obligations may cause conflict and confusion

The Framework appears to be based on a 'concurrency' regulation model in which enforcement powers are shared between an overarching regulator, the ACCC, and several sector-specific regulators.

There is a key difference between the proposed regime and other concurrency models (for example ASIC and ACCC powers to enforce contraventions of applicable consumer law) is that under those other models, there is predominantly a single set of obligations. In this case, there are multiple regulators, each administering a separate set of requirements. This may, in time, lead to potential conflict between the two sets of obligations, resulting in legal uncertainty. It also adds complexity as regulated businesses face potentially differing and varied compliance approaches from multiple regulators on the same issue.

It is also not clear how the penalty regime will work across the different sets of obligations. As mentioned above, there is overlap between the proposed ecosystem-wide obligations and the sector-specific obligations. It is therefore possible for the same conduct to result in a breach of the ecosystem-wide obligations and the sector-specific obligations. This is particularly concerning when there is potential for different penalties to apply at each level (and when the penalties for non-compliance under the CCA are extremely high). The penalty for a breach should be clear and should not depend on which regulator chooses to enforce compliance under which law. While we acknowledge the Government's intention to avoid two regulators taking action for the same conduct, we consider that a single, clear penalty regime administered by an appropriate industry regulator will avoid unnecessary complexity and uncertainty.

Given the evolving and complex nature of the online scams space, we suggest that a regulator with the necessary industry expertise be responsible for overseeing the development of the code. This is similar to the regulatory model adopted in other Australian contexts, such as the online safety space. ACMA, with its strong industry expertise, would be well-positioned to play this role.

Ensuring penalties are proportionate

As explained above, Meta is continually evolving systems and processes to identify and detect scams. Digital platforms are in a continual adversarial battle to stay ahead of new scams and circumvention techniques as they operate across the internet. Scammers are becoming increasingly sophisticated, may operate scams across multiple channels and continually take steps to evade detection.

In these circumstances, we have concerns that the existing CCA penalty regime is excessive and disproportionate. As we have explained, the Framework is in its early stages. A heavy-handed and excessive regulatory approach may not have the intended effect of incentivising industry to invest in the necessary measures to meaningfully address scams across the digital ecosystem. As we have outlined above, Meta already undertakes a significant, global effort to address the integrity of its products, in particular to address scams and fraudulent activity, and this activity is evolving as scammers continually adapt their techniques. We fully understand that a more prescriptive approach may be needed to combat scams, but a regime needs to be built on a clear evidence base. Given the early stages, we suggest a graduated approach to regulation and penalties that may arise, starting with industry-led codes which allow platforms to adapt their approach to scam detection and enforcement to ensure industry best practice. Similar to other regimes, serious penalties should be leveled for systemic or ongoing breaches.

In any event, to the extent that significant product builds are required, and particularly if the code departs from similar overseas obligations or existing systems, a significant grace period will be required before it takes effect.

Clarity needed on dispute resolution

We agree that consumer reports and complaint handling are an important element in scam detection. For digital platforms in particular, effective user reports can be a useful input for integrity measures to better detect and therefore enforce on scam activities as they evolve over time. In many of our education programs and on our services, we encourage consumers to use in-app reporting tools and via our help centers to report suspected scams.[49] These reports can provide important signals to our machine learning about potential violations of our policies which we can then apply to similar content resulting in scalable efforts to reduce scams. Over time, these reports help train our technology to be more accurate in proactively detecting and enforcing scams content. Any IDR regime should be flexible and allow these existing tools to be maintained and updated as a first line defence.

It is essential to our long-term business interest that users have a positive experience on our services and we recognise the importance of consumer oversight and greater accountability. This is why we have been expanding the ability of people to appeal our content decisions either to us directly for re-review or to the independent Oversight Board, which was established in 2020. This is also why Meta has supported the concept of a digital platforms ombudsman in Australia since it was first proposed in 2019.

The challenge, however, is how to design consumer protection mechanisms in ways that are genuinely effective, are practicable and which raise the bar on what is already provided. We suggest five key principles to guide the discussion to advance the development of the dispute resolution process:

- *Recognise existing and future innovations:* The models of customer service used by the digital industry represent some significant innovation in how to provide a good consumer experience at scale. Models like self-help centres and live chat have been pioneered by the digital industry and provide simple, user-friendly ways of resolving concerns that are used by significant numbers of people around the world every day.
- *Consider the complex nature of digital platform complaints:* Digital platform complaints are far more complex and cannot be viewed as equivalent to complaints in other sectors like telecommunications. Telecommunications complaints mostly centre around the quality of the service received, equipment or network faults, or billing issues; they are narrower in scope, whereas, for example, some consumer complaints about digital platforms are about other users and not even about the platform itself.
- *Complaints must be clearly scoped*: This could cover the full gamut of digital platforms' policies, could be related to data settings, and/or could relate to billing disputes. Each of these types of potential complaints is broad and highly complex.
- *Importance of separating out content issues from transactional issues*: There may be conflation or overlap between the two. For example, a user may claim that their social media account has been closed inadvertently. But actually, it is because they shared a piece of content that is classified as extremist or hateful under our policies or because they repeatedly shared content after receiving warnings that their use of the service would be restricted if they did not stop and there was no

[49] For example, Facebook, 'Report something', Help Centre, https://www.facebook.com/help/263149623790594; Instagram, 'How do I report a post or profile on Instagram?', https://help.instagram.com/192435014247952/?helpref=uf_share

financial loss incurred. It is important that content disputes such as these should not fall within the scope of the Framework and its obligations.

- *Consider the large number of existing channels:* There are a significant number of bodies who already raise concerns with Meta on behalf of consumers. We take a 'no closed door' approach, where we take referrals or concerns from a large number of government bodies regardless of whether it fits neatly with their remit.

Any IDR or EDR approach should take into account existing complaint resolution processes to facilitate the lowest cost point of resolving a dispute. This requires a review of existing reporting and complaint handling channels – both on platform and with existing regulators and ombudsmen. With respect to complaint handling and dispute resolution, there is already a robust and adapted Australian Consumer Law, the Privacy Act, and the Online Safety Act and most recently the NASC-- all of which are being used to apply scrutiny and accountability to digital platforms.

In principle, we support further consideration of complaint handling and IDR; however, it is difficult to comment in detail while this is the subject of future work under the ACCC Digital Services Platforms Inquiry (DPSI). While topic 5 of the DPSI considered an IDR and EDR mechanism for digital platforms, the scope, processes and mechanics of these measures remain unknown, making it challenging to comment on the Framework overall.

In order to provide further comments, it would be helpful to understand if the scope of the IDR and EDR contemplated would only relate to scams complaints or whether there would be a stand-alone dispute resolution mechanism, which would apply to a range of complaints, to which the Framework would refer. Similarly, any cross-over with existing complaint intake (we receive complaints via external sources including the NASC and ASBFEO) as well as an appropriate EDR facilitator with relevant industry knowledge, should also be considered as part of this exercise.

The importance of effective reporting obligations

We recognise the importance of information sharing across the scams ecosystem to ensure that all businesses can detect and prevent scams. However, it is important that the information sharing obligations under the Framework are clear, streamlined and effective.

The Framework imposes three obligations on businesses: (1) to report suspected or identified large-scale scam activity to other businesses, the NASC and relevant regulators; (2) to report emerging or cross-sectoral scam activity to other businesses, the NASC and relevant regulators where there is a significant risk to consumers; and (3) to respond to requests from the NASC or other relevant regulators for data on individual scam instances or reports, or actions taken in response. In addition, there is an obligation on digital platforms to identify and share information with other digital platforms and the NASC that an Australian user is or is likely to be a scammer.

It would be helpful to understand more about the evidence base that indicates that this level of reporting will be effective in driving investment by industry to reduce scams, as opposed to simply driving a compliance mindset that focuses on reporting for its own sake. There is a risk that such an obligation would cause businesses to share low quality or unverified information with other businesses simply to avoid non-compliance with the Framework. This would undermine the purpose of such information

sharing arrangements and detract resources away from combatting genuine scam activity. For this reason, Meta supports the NASC, taking a coordinating role with respect to the reporting of scam intelligence and the requirements for any intelligence sharing to be high-level and set to a level of detail and frequency that allow meaningful disclosures between industry and government. This would (1) ensure that intelligence reports benefit from the coordinating authority's efforts to investigate the veracity of reports and identify trends across sectors, and (2) assist in providing industry with clarity in relation to any obligations that may be triggered by the receipt of scam intelligence.

In addition, when imposing reporting and disclosure obligations on digital platforms such as these, it is important to consider that many of these platforms, including Meta, are headquartered in other jurisdictions such as the United States (US) and are subject to US laws. These laws limit the circumstances in which a US-based provider can disclose user information. This means that any obligation to share information about a specific Australian user is unlikely to be able to be fulfilled by US-based companies. Consequently, the Framework must deal with conflicts of law and not require providers to undertake any actions that may result in a breach of any applicable foreign laws. In our view, this is appropriate and necessary so platforms are not in a 'Catch-22' situation whereby they are forced to choose between either breaching the obligation under the Framework or breaching another law by which they are bound simply because of the impossibility of complying with both.

Given this, any new reporting obligations need to be carefully calibrated to be practical and effective for combating scams.

With respect to the proposed anti-scams strategy obligation, Meta has already made significant investments in our integrity measures and in providing transparency and accountability around these. It is not clear that the development of an anti-scams strategy in the manner proposed would add to the overall effect of the Framework in addressing scams in Australia. The highly adversarial and rapidly evolving nature of scams requires companies like Meta to be constantly adapting our anti-scam strategies. In this context, we are concerned that legislating and formalising the development and review of a company's anti-scam strategy with high-level sign-off would not prove effective in reducing the number of scams targeting Australians and that rather, it would impose a considerable compliance burden requiring significant time and resources that could otherwise be directed towards more effective prevention and deterrence efforts.

Complexities and dynamics of the digital space

When considering both the overarching framework but also the sector specific code with respect to digital platforms, it is important to understand the complex and highly dynamic nature of the digital space and the ways in which scammers quickly adjust their tactics to evade detection. This means that any regulatory framework must contain sufficient flexibility to allow tactics and responses to scams to quickly adjust and adapt.

As our Community Standards Enforcement Report makes clear, enforcement can fluctuate due to the highly adversarial nature of the online environment. For example, accounts actioned for being fake (often a tactic used by scammers) increased from 676 million in Q2 2023 to 827 million in Q3 2023.[50]

[50] Meta, 'Community Standards Enforcement Report Q3, 2023', Transparency Centre, https://transparency.fb.com/reports/community-standards-enforcement/fake-accounts/facebook

As companies such as Meta and the broader industry take action to disrupt scams and malicious behaviour, threat actors rapidly evolve their tactics in attempts to evade detection and enable persistence. One way they do this is by spreading across as many platforms as they can to protect against enforcement by any one service. These changes are likely an attempt by threat actors to ensure that any one service has only limited visibility into the entire operation. When bad actors count on us to work in silos while they target people far and wide across the internet, we need to work together as an industry to protect people. The practical impact from this when designing digital sector specific obligations is that it may not always be possible for one digital platform to see all aspects of a scam and take the final last step to prevent it.

Additionally, it is important that any obligations are balanced and proportionate, recognising that the vast majority of interactions between consumers and businesses online are positive. Digital platforms have democraticised e-commerce, by providing businesses (especially small businesses) with easy-to-use, no- or low-cost entry points for digital transformation, which they can then build on to advance their business growth. For example, a 2023 report by ThoughtLab found that two-thirds of surveyed Australian small and medium-sized enterprises credited Meta platforms with helping them start up their business.[51] By applying numerous obligations on businesses to use the free tools provided by digital platforms, that are not demonstrated to be effective to target scammers, the Proposed Framework risks adding unnecessary friction to the digital economy and putting Australian businesses at a disadvantage, given the Proposed Framework is more onerous than that contemplated in other jurisdictions, such as the UK.

This background means that it is important that any requirements for small businesses to use the free and advertising tools available on digital platforms are not unduly burdensome, and are demonstrated to be effective in thwarting scammers.

[51] ThoughtLab, 'The Digital Journey of SMEs in Australia - How small and medium-sized enterprises drive business and economic results through digital innovation', May 2023, https://thoughtlabgroup.com/the-digital-journey-of-smes-in-australia

Table of Responses to Stakeholder Specific Questions

No.	Question	Summary of Meta Response
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?	Meta recognises and supports the intent of the Framework. However, we have the following concerns and suggestions relating to the structure, obligations and enforcement mechanisms proposed in the Consultation Paper: Implementing the Framework at this time is premature. Given that the establishment of the NASC and industry and the Government's increased anti-scam measures are still nascent, it is as yet too early to design and implement a full, evidence-based regulatory framework. We suggest that further time be taken to review and consider the data and evidence of what works and where gaps remain to more effectively combat scams. Meta suggests the overall approach of industry-led codes intended to establish consistent baseline obligations across the sector and provide a basis for more effective coordination among industry and with regulators. We also endorse the role of ACMA in relation to a potential digital platforms code, as a regulator with significant expertise in this space. DIGI, with its experience in code development, would be well situated to lead this process on behalf of the digital industry. The proposed structure of the Framework is duplicative with primary law and sector-specific code obligations and is in some respects too vague to be capable of providing certainty for industry in terms of implementation, reporting and enforcement. It is not clear where more is needed nor the precise roles and responsibilities for each stakeholder within the ecosystem. This is a further indication that the Framework is premature and risks diverting investment away
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?	
3.	Are the legislative mechanisms and regulators under the Framework appropriate, or are other elements needed to ensure successful implementation?	

		from detecting and enforcing on scam activity, and incentivising industry to prioritise regulatory compliance over further innovation to disrupt and deter scams. With particular respect to the overarching regime in the *Competition and Consumer Act 2010* (CCA), we encourage the Government to carefully review whether it is necessary and proportionate. The proposed obligations in the overarching regime appear duplicative in many respects with the potential sector specific obligations. We suggest that the regime should be designed with the benefit of a clear assessment of (a) existing industry efforts to target and prevent scams, (b) industry best practice in this area, especially where scams are conducted online and across different platforms, (c) the best form of cross-industry and industry-government collaborations and (d) any gaps or deficiencies in the NASC capabilities. We see significant benefits in a central body, such as the NASC or the ACCC, taking a coordinating role between the Government, law enforcement and the private sector. In particular, this coordinating body could receive and investigate scam reports (from consumers, government, law enforcement and the private sector) and share intelligence (or content takedown requests) as appropriate to disrupt scams. This would also assist in providing industry with clarity in relation to any obligations that may be triggered by the receipt of scam intelligence (for example, the obligations in the primary law to verify and trace scams, and to take steps to disclose to a consumer they may be a target of scam). We also encourage the Government to review the need for multiple regulators enforcing compliance with private sector obligations under the Framework - including overlapping obligations under the primary law and the industry codes. In our view, the current delineation between the two is duplicative and confusing. It is also important to consider the scope of these overlapping obligations in the context of the very significant proposed penalties - the greater of $50 million, 3 times the value of the benefit obtained, or 30% of the corporations' adjusted turnover during the breach - in addition to potential penalties under the proposed industry codes.

		Please see our *General Comments on the Proposed Scams Framework* for further details.
4.	Does the Framework provide appropriate mechanisms to enforce consistent obligations across sectors?	Through the NASC, the Government has successfully brought together the banking, telecommunications and digital industries and increased collaboration across these industries to do more to combat scams targeting people in Australia. This process should be allowed to run and take proper effect, so that specific and proportionate cross-sectoral obligations can be identified and then standardised.
5.	Is the Framework sufficiently capable of capturing other sectors where scams may take place or move to in the future?	Meta supports the intention of developing a Framework that is flexible and responsive to future changes in the scams ecosystem. We encourage the Government to carefully consider the criteria that should be applied by the Minister in making decisions to designate particular sectors or subsectors covered by the Framework. We would also encourage opportunities for industry consultation on sectors/subsectors proposed to be designated. We note that it is not yet clear how the Framework will apply to other sectors that may also play a key role in the creation and commission of scams, such as dating sites, cryptocurrency exchanges, superannuation funds, and payment service providers. Analysis of ACCC scams data and trends may be useful in identifying whether these, or any other sectors, should also be brought under the Framework.
6.	What future sectors should be designated and brought under the Framework?	
7.	What impacts should the Government consider in deciding a final structure of the Framework?	Similar to our response to Questions 1-3 above, it is our view that in deciding the final structure of the Framework, the Government should consider the data and evidence of what is needed to be done by industry to play its part in combating scams, as well as what types of Government interventions are effective to achieve this. In light of the nascency of industry's and the Government's new anti-scam initiatives, we suggest that more time be given to develop the Framework, in order to ensure that all its aspects and the digital sector-specific obligations are informed by evidence, practicable and effective to combat scams. Please see our *General Comments on the Proposed Scams Framework* for more details.

Questions on definition		
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?	The proposed definition of 'scam' - '*a dishonest invitation, request, notification or offer, designed to obtain personal information or a financial benefit by deceptive means*' - is overly broad. Given the extent of the proposed penalties, complexity of regulators and vagueness of proposed internal and external dispute resolution mechanisms, the definition needs to be more tightly scoped to be workable, effective and proportionate. Specifically, we suggest removing 'personal information' from the proposed definition, on the basis that scams are financially motivated and designed to secure personal benefit rather than personal information (the latter of which tends to be a privacy breach). This would avoid conflating the issue of scams with issues relating to privacy and data breaches, and the risk of setting unclear and confusing obligations that are unable to be effectively implemented. Greater clarity should be provided around certain concepts in the definition (such as "designed to"). It would also align with Meta's relevant policies, which focus on content and behaviours that purposefully intend to deceive, willfully misrepresent or otherwise exploit others for money or property, including content that seeks to coordinate or promote such activities using our services. It would also align with the UK Online Fraud Charter, which focuses solely on financially motivated fraud and deception.[52] Please see our comments in the *General Comments on the Proposed Scams Framework: Clarifying the proposed definition of a 'scam'* section above. The development of an industry-led code of conduct with co-regulatory design, consistent with our recommendation in our *General Comments on the Proposed Scams Framework* section above, will allow benchmarking of a consistent definition across online services.
9.	Does a 'dishonest invitation, request, notification, or offer' appropriately cover the types of conduct that scammers engage in?	
10.	Does the proposed definition of a scam appropriately capture the scope of harms that should be regulated under the Framework?	
11.	What impacts should be considered in legislating a definition of a scam for the purposes of this Framework?	

[52] UK Government, Online Fraud Charter, 30 November 2023, https://www.gov.uk/government/publications/online-fraud-charter-2023

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?	We support a broad definition of "digital communication platforms" that captures all common methods of scammer communication with users. Please see our response to Question 14 below.
13.	Should the definitions of sectors captured by the Framework be set out in the primary law or in the industry-specific codes?	Consistent with our recommendation in our *General Comments on the Proposed Scams Framework*, the obligations – including the definition of sectors to be captured by the Framework – should be set out in an industry-led code of conduct with co-regulatory design.
14.	What impacts should the Government consider in deciding the definitions of digital communications platform or ADI?	Recognising that all stakeholders that are part of the scams ecosystem - including business, users, government and law enforcement - have a role to play in combating scams, Meta supports a broad definition of digital communications platform that would capture all common methods of scammer communication with consumers. For example, Scamwatch lists a number of common digital platform delivery methods such as email, 'internet', social networking, and mobile applications.[53] Moreover, as threat actors are enforced against, they evolve their tactics to evade detection and spread across as many platforms as possible. In order to be effective, it is therefore important that the digital sector-specific code is wide-ranging across the digital industry. We recognise that different digital platforms deliver a very broad range of services. For example, a social media platform (like Facebook, TikTok or Snap), an encrypted messaging platform (like WhatsApp or iMessage), a search platform (like Google or Bing), an email platform (like Gmail or Outlook) and a video platform (like YouTube) differ in multiple dimensions, as may the common scam types and characteristics on each platform, and the available detection and enforcement techniques. Each of these services may also have marked differences in the manner of communication provided - e.g. on a one-to-one, one-to-many, or end-to-end encrypted basis. All of these service distinctions may necessitate differences in approach to obligations (for

[53] National Anti-Scam Centre, 'Scam statistics', *Scamwatch*, https://www.scamwatch.gov.au/research-and-resources/scam-statistics

		example through sub sector codes), and further highlight the need for development of obligations to be industry-led in order to be effective, responsive to the harm at issue and adaptable in a space of rapidly evolving harm archetypes.
Questions on overarching principles-based obligations		
15.	Are there additional overarching obligations the Government should consider for the Framework?	The Government should consider – Instead of introducing a code of conduct within the CCA – the development of an industry-led code of conduct with co-regulatory design, consistent with our recommendation in our *General Comments on the Proposed Scams Framework*.
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 scams related record-keeping?	The Framework would benefit from a greater review of the evidence of what steps are needed to be taken by industry to combat scams, especially given the adversarial, cross-border and evolving nature of scams. It is not clear, for example, that legislating specific actions such as internal processes for the development of an anti-scams strategy or scams-related record-keeping – will incentivise the appropriate investment by industry in greater scams prevention versus investment in compliance. Instead of introducing these obligations within the CCA, the development of an industry-led code of conduct with co-regulatory design, consistent with our recommendation in our *General Comments on the Proposed Scams Framework* section above, will address this concern. On the question of whether there should be fixed timeframes, we note that digital platforms can best address harmful conduct and content on our services when there is flexibility in determining where to allocate resources and investments that will maximise their safety and integrity efforts. Requirements that impose fixed timeframes to take specific actions incentivise companies, instead, incentivise industry to prioritise regulatory compliance over promoting a safer and more secure ecosystem, which may lead to unintended, adverse consequences. For example, requiring platforms to respond to user reports within a fixed number of hours is not only highly impractical and operationally infeasible, but also fails to solve the problem of reducing harmful or problematic content on platforms. It can often be the case that user

		complaints do not come with sufficient information or evidence of an offense, which is necessary for service providers to process and review under their global processes. Digital platforms have limited ability to investigate such user reports, as they do not have the investigative powers of a court or a government authority to gather necessary information. In these circumstances, setting arbitrary timeframes becomes meaningless. Additionally, not all user reports are equal in the level of risk and harm it may cause. Some reports may be benign, where there is no immediate harm or there are no or only a small number of views, while other posts may be spreading rapidly and pose a greater harm to individuals. Requiring platforms to treat all reports equally and have them blocked within a fixed period of time risk unintended, adverse consequences, such as: ● Forcing companies to be less diligent with the review processes in order to meet fixed timeframes, which may lead to over-enforcement and the stifling of free expression. ● Forcing companies to treat all user reports equally, rather than prioritizing reports that may pose a greater harm to an individual. It is important to balance expediency with the risk of harm and rights of users. As a data point, a report by the CCIA Research Center on the experience of Germany's Network Enforcement Act (NetzDG) — which mandated digital platforms block or remove user-reported illegal content within 24 hours if manifestly unlawful — noted that over 84% of user complaints filed were false positives and over 99% were non-violative content or duplicative.[54] Compliance with NetzDG required a significant amount of resources to review millions of user reports, which was disproportionate to the number of pieces of content reported that were actually illegal and blocked.
17.	Do the overarching obligations affect or interact with existing businesses objectives or mandates around efficient	Yes. We are concerned that the overarching obligations – particularly given the overly broad definition of a 'scam', the substantial penalties and

[54] Computer & Communications Industry, Government Mandates to Remove Content are Ineffective, Costly, and Anti-Competitive, 18 April 2023, https://research.ccianet.org/reports/ccia-netzdg-german-network-enforcement-act-report

	and safe provision of services to consumers?	the lack of clarity relating to some obligations (for example the development of anti-scam strategies) – risk creating additional burdens that will incentivise industry to focus on compliance, rather than further improve and innovate on scam prevention. Instead of introducing these obligations within the CCA, the development of an industry-led code of conduct with co-regulatory design, consistent with our recommendation in our *General Comments on the Proposed Scams Framework* section above, will address this concern.
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?	Meta recognises the importance of transparency and accountability. However, reporting must be tempered so as not to distract resources and investment from combatting scams and protecting the integrity of services, recognise the extensive existing voluntary transparency efforts and existing reporting obligations under many other schemes, and also recognise conflict of laws. Meta would support the National Anti Scams Centre / Australian Competition and Consumer Commission or another central body taking a coordinating role with respect to reporting of scam intelligence across multiple sectors (and in coordination with the Government and law enforcement), provided that it was high level trends insights. This would (1) ensure that intelligence reports benefit from the coordinating authority's efforts to investigate the veracity of reports and identify trends across sectors, and (2) assist in providing industry with clarity in relation to any obligations that may be triggered by the receipt of scam intelligence. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: The importance of effective reporting obligations*.
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?	There is a risk that the Framework will incentivise compliance with the obligations it proposes, with significant penalties, rather than investment in combating scams. There are a number of highly prescriptive obligations that do not appear to be evidenced based and targeted to prevent scams. Please see our comments above in the sections titled *General Comments on the Proposed Scams*

		Framework.
Questions on anti-scams strategy obligation		
20.	What additional resources would be required for establishing and maintaining an anti-scam strategy?	Companies such as Meta have made significant investments in integrity measures and in providing transparency and accountability for these, as our Transparency Center makes clear. It is not clear that the development of an anti-scam strategy in the manner proposed will be additive and further the goals of the Framework, as opposed to distracting resources from the work needed to combat scams. Please see our comments above in the *General Comments on the Proposed Scam Framework: Framework should be fit-for-purpose & evidence based* section above.
21.	Are there any other processes or reporting requirements the Government should consider?	In assessing the measures required under the proposed Framework, we encourage the Government to leverage its considerable investment in the NASC to identify the evidence, data and gaps to inform the development of obligations, and to allow additional industry initiatives such as Meta's existing and new anti-scam initiatives to take effect. Please see our comments above in the *General Comments on the Proposed Scam Framework*
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?	Meta provides significant resources to raise awareness by consumers of scams and partners with a wide range of organisations to ensure that consumers, who are unable to use on-platform measures, can secure the resolution needed. Given the highly adversarial nature of scams, care must be taken before any measures are released publicly. Additionally, Australia has robust consumer protection laws and any further obligations should be calibrated against existing requirements under these laws.
23.	How often should businesses be required to review their anti-scam strategies and should this be legislated?	Meta makes significant investments in policies, technology, transparency, partnerships and consumer awareness campaigns to combat scams. The highly adversarial and rapidly evolving nature of scams requires companies such as Meta to be constantly adapting our anti-scam strategies on a daily basis. Such regulatory obligations come at a significant time and resource cost. We are concerned that formalising and legislating the development and review of a company's
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?	

		anti-scam strategy with high-level sign-off would not be effective in reducing the number of scams targeting Australians. Instead, it would incentivise a compliance approach by industry at the expense of a more effective prevention and deterrence approach. Please see our comments above in the *General Comments on the Proposed Scam Framework: Framework should be fit-for-purpose & evidence based* section above.
25.	What level of review and engagement should regulators undertake to support businesses in creating a compliant anti-scam strategy?	In establishing the NASC, the Australian Government has taken a leading step forwards towards bringing together industry and governments to increase their collaboration and signal the need for industry to do more to combat scams targeting Australians. This process should be allowed further time to run, so that the Government can better identify how it can support businesses to do more to create anti-scam strategies.
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?	Meta invests significant resources in providing industry-leading transparency. We have also increased our collaboration with the Australian banking sector and are working to respect the intent of the Government's Proposed Framework, to step up our work to combat scams targeting Australians. Any additional information sharing should be evidence-based and identified as effective and efficient in enabling the greater prevention of scams, rather than incentivising a compliance approach at the expense of a prevention and deterrence approach, and be consistent with applicable laws that apply to US-based companies. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: The importance of effective reporting obligations*.
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?	There are significant limitations on information sharing. First and foremost are the legal obligations that apply to US-based companies that prevent the sharing of user communications. Secondly, information sharing should focus on high priority risk of scams content, upon mutually-agreeable volume, and take into

		consideration different companies' existing systems and processes in handling scams intelligence reports. The data sharing collaboration should also not come at the expense of the time and resources that companies need to handle their day-to-day anti-scam operations, such as responding to user reports. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: The importance of effective reporting obligations*.
28.	What other information sharing arrangements exist that the Government should consider/leverage for the implementation of the Framework?	All information sharing by Meta is consistent with our commitment to provide meaningful data that does not in turn arm scammers and other malicious actors to misuse that information to adapt and further hone their craft. To ensure prompt and meaningful action by Meta on any information shared with us, it is important that it is shared in a format and with the requisite details that allow us to act. This is why we invest in on-platform reporting tools, have established escalations channels with a number of organisations including the ACCC's Scamwatch, and in the process of piloting a direct reporting channel with the Australian banking industry. These measures allow us to ingest higher quality reports that we can action promptly and use to identify what additional measures we can take to increase our detection and prevention of scams on our services. Any additional information sharing measures should be carefully calibrated to ensure meaningful transparency and actionable intelligence, without leading to more informed scammer behaviour. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: The importance of effective reporting obligations*.
29.	Are there any impediments to sharing or acting on intelligence received from another business or industry bodies?	
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?	IDR reform proposals lack specificity. The ACCC reports on which this recommendation is based contain only generalised statements, without examples or clear insights for service providers such as Meta to identify problems and possible

		solutions, or what the IDR reforms being contemplated might entail. This makes it challenging to respond to this question. With respect to the EDR scheme, It is important that the complaints handling scheme is developed following best practice regulatory principles, in line with those articulated by regulation experts such as the Productivity Commission, the OECD, COAG and the Australian Government Guide to Regulation. Specifically, it must be evidence based, necessary, fit-for-purpose, proportionate, and independently assessed for effectiveness. It is difficult to engage with this proposal without understanding or inputting into the procedural parameters of such a body. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: Clarity on dispute resolution*.
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?	It seems premature to discuss these issues given the proposed EDR schemes with respect to digital platforms has not yet been scoped, let alone finalised. Meta has consistently expressed support for an ombudsman scheme in principle, but noted that a lot depends on the detail of how it would be implemented and specifically, with respect to which type of complaints given that there are various other complaint and appeal mechanisms available to Australian consumers with respect to Meta's services. At present, it is not clear who would manage the EDR with respect to digital platforms,how that body would have the requisite industry expertise and knowledge to determine if a business has breached its obligations under the framework and in which circumstances a platform may be required to provide redress and what that redress may look like. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: The importance of effective reporting obligations*.
32.	Should the Government consider	Please see our response to Question 31. It seems

	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?	premature to be considering this.
33.	Does the Framework set out a clear pathway for compensation to consumers if obligations are breached by regulated businesses?	No, given the vagueness of the IDR and EDR proposals, it seems premature to be discussing pathways for compensation for consumers.
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?	No, the sector specific obligations should be informed by evidence that the obligations will direct effective integrity and compliance investment in the problem space, endure in a landscape of rapidly changing harm archetypes and by simple and comprehensible to enforce. These obligations should be informed by data from the NASC and the results from additional measures being adopted by industry and fed into an industry-led code overseen by the ACMA. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: Proposed obligations are inflexible & potentially duplicative* and *General Comments on the Proposed Scams Framework: Concurrent regulator approach with overlapping obligations risks conflict and confusion*.
35.	Are there additional obligations the Government should consider regarding the individual sector codes?	Any sector specific obligations should be informed by evidence-backed inputs from industry. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: Proposed obligations are inflexible & potentially duplicative* and *General Comments on the Proposed Scams Framework: Concurrent regulator approach with overlapping obligations risks conflict and confusion*.
36.	Do the obligations considered for each sector reflect appropriate consistency across the scams ecosystem?	Please see our comments in response to Question 35.
37.	Are the proposed obligations for the sector-specific codes set at the right level, sufficiently robust, and flexible?	Please see our comments in response to Question 35.
38.	Are the proposed approaches to	The Consultation Paper notes two possible

	developing sector-specific codes appropriate, and are there other approaches that could be considered to meet the objectives of the Framework?	pathways to the development of a digital platform industry code - (1) ACMA developing mandatory industry standards in consultation with industry, or (2) industry developing a code to be registered and enforced by ACMA. In order to be implementable and effective, the development of a digital platform code will need to be heavily industry-led to ensure that all obligations are technically feasible and able to be implemented within a reasonable timeframe to meet the objectives of the Framework in addressing scams. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: Proposed obligations are inflexible & potentially duplicative* and *General Comments on the Proposed Scams Framework: Concurrent regulator approach with overlapping obligations risks conflict and confusion*.
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?	No, requirements that impose fixed timeframes to take specific actions incentivise companies, instead, to prioritise regulatory compliance over promoting a safer and more secure ecosystem, and may lead to unintended, adverse consequences. For example, requiring platforms to respond to user reports within a fixed number of hours is not only highly impractical and operationally infeasible (because more context may be needed to properly assess a complaint), but also fails to solve the problem of reducing harmful or problematic content on platforms. The experience within the digital industry is that user complaints may not come with sufficient information or evidence of an offense which is necessary for service providers to process and review. Digital platforms have limited ability to investigate such user reports, as they do not have the investigative powers of a court or a government authority to gather necessary information. In these circumstances, setting arbitrary timeframes prioritises action over thoughtfulness. Additionally, not all user reports are equal in terms of the level of risk and harm it may cause. Some reports may be benign, where there is no immediate harm or there are no or only a small number of views, while other posts may be

		spreading rapidly and pose a greater harm to individuals. Requiring platforms to treat all reports equally risk unintended, adverse consequences, such as: ● Forcing companies to be less diligent with the review processes in order to meet fixed timeframes, which may lead to over-enforcement and the stifling of free expression. ● Forcing companies to treat all user reports equally, rather than prioritising reports that may pose a greater harm to an individual. It is important to balance expediency with the risk of harm and rights of users. If a timeframe should be specified, we recommend that flexibility is included to allow for what is reasonable, having regard to the context and complexity of the content being reported. A report by the CCIA Research Center on the experience of Germany's Network Enforcement Act (NetzDG) — which mandated digital platforms block or remove user-reported illegal content within 24 hours if manifestly unlawful — noted that over 84% of user complaints were false positives and over 99% were non-violative content or duplicative.[55] Compliance with NetzDG required a significant amount of resources to review millions of user reports, which was disproportionate to the number of pieces of content reported that were actually illegal and blocked.
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?	There is a risk that the Framework will incentivise compliance with the obligations it proposes, with significant penalties, rather than investment in combating scams. There are a number of highly prescriptive obligations that do not appear to be evidenced based and targeted to prevent scams. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework: Proposed obligations are inflexible & potentially duplicative* and *General Comments on the Proposed Scams Framework: Concurrent regulator approach with overlapping obligations risks conflict and confusion*.

[55] Computer & Communications Industry, *Government Mandates to Remove Content are Ineffective, Costly, and Anti-Competitive*, 18 April 2023, https://research.ccianet.org/reports/ccia-netzdg-german-network-enforcement-act-report

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?	In order to be implementable, effective and efficient, we suggest that further work should be conducted with industry representatives to develop sector-specific sets of requirements, with the benefit of industry expertise and co-regulatory design.
42.	Are there additional areas the Government should consider in ensuring appropriate interaction between the bank-specific scams code and the ePayments Code?	Not applicable
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?	See response to Questions 1-3. We also note that a key difference between the proposed regime and other multi-regulator models is that under those other models, there is predominantly a single set of obligations. By contrast, under the Framework, there would be one set of 'principles-based' obligations under the CCA and a different set of obligations under a sector-specific code, each with potentially different penalties and being enforced by different regulators. This complexity is likely to lead to confusion and conflict, in particular where different regulators adopt different approaches to similar obligations. For this reason, we do not support a multi-regulator approach and instead support an industry-led code enforced by ACMA. Please see our comments above in the section titled *General Comments on the Proposed Scams Framework.*
44.	Are there other factors the Government should consider to ensure a consistent enforcement approach?	
45.	Should the penalties for breaches of sector-specific codes, which sit in their respective sector legislation, be equal across all sectors?	