# Scams – Mandatory Industry Codes

Westpac Banking Corporation

**January 2024**

WE ARE WESTPAC GROUP

# INTRODUCTION

Thank you for the opportunity to provide feedback on Treasury's Scams Mandatory Industry Codes Consultation Paper (Consultation Paper). Keeping Australians safe is a critical national priority, and this includes protecting Australians from scammers. Westpac supports the introduction of a robust and balanced anti-scams regime to make Australia a harder target for scam activity.

While there are many enablers and drivers of scams across the economy, the impact of scams cuts to the core of our commitment to customer care. As scammer activity has increased over the past few years, Westpac has responded by investing in new detection capabilities and customer-facing measures designed to prevent scam losses. Westpac has invested upwards of a hundred million dollars over the past two years to better protect our customers from scams and in this time has prevented over $400 million from being lost to scammers, with new initiatives in development for delivery in 2024[1].

Scam prevention, detection and response is a complex, nuanced and ever-evolving undertaking, set to become increasingly challenged by the rapid acceleration of AI technology. But with the right policy settings in place, Australia has an opportunity to introduce a world-leading whole-of-ecosystem approach with strong defences in place across the economy.

We remain committed to playing a key role in the fight against scammers.

[1] Refer to Appendix 1 for examples of Westpac's scam protection measures.

## SUMMARY

Westpac broadly supports the principles and Framework being proposed by the Government, subject to some refinements we believe are critical to giving full effect to the ecosystem approach to addressing scams (a foundational intent of the proposed Framework). In our view, the biggest risk within the proposed regime is the potential creation of a lopsided ecosystem which does not equally distribute accountability and responsibility across its industry participants. Such an outcome would expose consumers to what otherwise would be an avoidable risk where defences remain weaker in the ecosystem chain and compromise the policy intent.

It is Westpac's submission that all sectors require equal levels of investment, vigilance and regulatory oversight. Otherwise, Australia's new scams regime could be likened to an unseaworthy vessel with holes in the hull (some easily visible and some not).

The recommendations outlined in this submission are designed to:

- Put customer experience at the centre of the Framework's architecture;
- Suitably incentivise scam prevention and deterrence across the entire scams ecosystem; and
- Deliver consistent outcomes and obligations for regulated industry sectors.

In addition to the three guiding principles identified in the Consultation Paper ("whole-of-eco-system approach"; "flexible and responsive"; and "leveraging existing regimes"), Westpac supports as a foundational objective the need to avoid inducing moral hazard. Put simply, scammers should not be rewarded for their criminal activity. As Assistant Treasurer and Minister for Financial Services Stephen Jones correctly identified, there is a need for policy makers to avoid simplistic models that create a honey pot of funds for scammers[2]. Instead, we should harness the opportunity to become a world leader by introducing a whole-of-ecosystem approach that will ultimately provide better, as well as more sustainable and responsive protection, for the Australian public.

### RECOMMENDATIONS

We make six recommendations for Government's consideration:

- **Recommendation 1:** Appoint a single industry scams ombudsman to undertake external dispute resolution for all sectors, and uplift internal dispute resolution processes across industries. We are of the view that the Australian Financial Complaints Authority (AFCA) is best placed to play this role.
- **Recommendation 2:** Appoint a single scams regulator (the Australian Competition and Consumer Commission (ACCC)) to enforce all cross-sector industry codes (as opposed to a multi-regulator model) and ensure regulatory efficiency and consistency.
- **Recommendation 3:** Apply sector-specific obligations which achieve genuine uplift of existing industry practice across all sectors.
- **Recommendation 4:** Accelerate the delivery of Government's SMS Sender ID Registry.
- **Recommendation 5:** Bring crypto exchanges and online marketplaces into the ecosystem as soon as possible.
- **Recommendation 6:** Use a pragmatic but flexible definition of scams, which draws a definitive line between scam and fraud activity.

[2] https://www.afr.com/politics/scams-out-of-control-but-no-move-to-force-banks-to-bail-out-victims-20221104-p5bvoi

# RECOMMENDATIONS

## Recommendation 1:

*Appoint a single industry scams ombudsman (AFCA) to undertake external dispute resolution (EDR) for all sectors and uplift complaints frameworks as well as internal dispute resolution (IDR) processes across industries.*

The primary consideration underpinning the Framework's EDR design should be customer experience. The process should be clear on where to go, it should deliver consistent outcomes for similar cases, and it should be easy to navigate once a dispute has started, negating the need for complex and timely referrals between the ecosystem sectors.

The establishment of a single industry scams ombudsman to deal with disputes spanning the ecosystem would provide consumers with one front door to make complaints. Consistent with the Framework principle of "leveraging existing systems and processes", Westpac submits that AFCA is best placed to undertake a new expanded dispute resolution role for all regulated sectors.

In addition to the consumer benefits described above, advantages of this approach include:

- Delivering consistent outcomes for similar cases, ensuring fairness and robustness across sectors.
- Negates the need to establish either a new government body or create new sector-specific bodies (e.g. for digital platforms).
- Avoids having to establish a complex process/scheme to knit multiple ombudsman schemes together under a split model, to determine how the scam materialised across the ecosystem and whether sectors have complied with obligations.
- Leverages existing model maturity. Unlike the Telecommunications Industry Ombudsman, AFCA already has extensive expertise in managing scams disputes.
- Efficiency and ease of incorporating other sectors. AFCA's present remit already extends across relevant sectors (e.g. banking, superannuation, payments and crypto exchanges). Furthermore, AFCA's remit is likely to extend to new sectors in the digital payments and crypto sectors as part of Treasury's concurrent consultation on Australia's payments system reform.
- Scams-related customer complaint matters often have co-existing issues in areas that already fall within AFCA's existing remit.
- This approach best meets the stated Framework objectives: "leverage existing regimes"; "whole-of-ecosystem approach"; and "flexible and responsive framework".

In forming our recommendation that AFCA is best placed to undertake whole-of-ecosystem dispute resolution, Westpac consulted with external stakeholders to understand the views of those closest to the harm caused by scams. We also note this structure would significantly expand AFCA's role and caseload and therefore would need an appropriate ecosystem-wide funding model, along with increased telco and digital platform sector expertise, to support its expanded role.

**Internal Dispute Resolution (IDR)**

A single ecosystem wide EDR scheme will need to be supported by a similarly efficient and thoughtfully designed IDR process. This is a challenging proposition within an ecosystem model as presently, only banks are subject to the most stringent IDR obligations.

One suggestion to achieve ecosystem uniformity of IDR systems, and thereby uniformity of customer experience, is to replicate and apply existing best practice IDR standards to all sectors. For example, this could be achieved by setting the existing requirements under RG271 to be the ecosystem standard for IDR processes. This would set a high benchmark for consumer dispute resolution, it would avoid the requirement to design and build a new model, and it would ensure all IDR processes across all entities meet the same high bar. Another example could be to use the approach taken to IDR in relation to subscribers who are not AFS licensees under Appendix A of the ePayments Code (having said this, we note Appendix A is RG 271 "lite" and if adopted for scams would require some enhancements).

While consumers may look to banks as the default entry point for IDR, there are very few scams that don't first involve other ecosystem players (see Figure 1). This is why a coherently designed process which applies responsibility to all sectors is important from a consumer standpoint. It is also essential that individual IDR structures don't result in a system where consumer complaints are 'forum shopped' across the ecosystem, and banks should become the quasi-ombudsman or an adjudicator of responsibility across the sectors. We believe this is a highly possible consequence of a siloed IDR model.

***Figure 1: Scam types mapped to most likely source of origin***

| Scam type | Most likely source of origin |
|---|---|
| Investment | Digital platform (e.g. internet searches or advertisements) |
| Romance | Social media platform |
| Unexpected money | Social media platform or telecommunication |
| Buying & Selling | Digital or social media platforms (e.g. online retailers or marketplaces, fake websites) |
| Threat & Penalty | Telecommunication (e.g. cold call from a scammer) |
| Job scam | Digital and social media platforms |
| Impersonation scam | Telecommunication and social media platforms (e.g. messaging services or apps) |

We believe further development of a draft system would benefit from a joint ecosystem working group, which could be tasked by Government with agreeing and finalising a design. In our view, this model best meets the stated Framework objective of "whole-of-ecosystem approach".

## Recommendation 2:

*Appoint a single scams regulator (the ACCC) to enforce all mandatory cross-sector codes (as opposed to a multi-regulator model).*

While we acknowledge sectoral regulators have existing relationships, Westpac is not supportive of the multi-regulator approach outlined for consideration in the Consultation Paper. The proposed approach seems contrary to the Framework's "whole-of-ecosystem approach" objective by embedding sectoral silos rather than creating a true ecosystem model.

Specifically, the proposed regime does not adequately mitigate the risk of regulators having different powers, enforcement priorities, and cultures.

In our view, the best approach is for Government to pursue regulatory symmetry by avoiding regulatory overlap to the extent that this is possible, with the ACCC assuming ecosystem-wide responsibility for scams. This is consistent with Government's establishment of the National Anti-Scam Centre (NASC) and best meets the stated Framework objectives: "leverage existing regimes"; "whole-of-ecosystem approach"; and "flexible and responsive framework".

The ACCC presently has experience and expertise in all scam types, has carriage of the NASC, and has an existing remit and engagement with banks, telecommunication providers and digital platforms.

A single regulator with one EDR approach installs simplicity and remains consistent with the foundational premise of the Government's anti-scams Framework.

## Recommendation 3:

*Apply sector-specific obligations which achieve genuine uplift of existing industry practice to all sectors.*

While there will be necessary variations between sectors, the sector-specific obligations should be uniform or like-for-like as far as practicable, to give proper effect to ecosystem-wide scam prevention measures. For the ecosystem to be genuine, the scams framework must assign responsibility evenly across the sectors. It is our submission that all participants require uplift.

### Verification and authenticity

A key enabler of many scams is the ability for scammers to hide or assume a different identity. Scam prevention could be greatly bolstered by enhancing trust and verification practices across the digital landscape – not just in banking.

At the heart of the banking industry's proactive commitment to reducing scams is a $100 million investment in new payee verification technology to be rolled out across all Australian banks[3]. This will help customers verify the account name recorded against the BSB / account number and mitigate the risk of consumers being manipulated into paying a scammer. This is a significant technological undertaking demonstrative of the banking industry's commitment to tackling scams and building trust in the digital era.

Through the Australian Banking Association's (ABA) Scam-Safe Accord, Westpac has also committed to introducing biometric checks for new individual customers opening accounts online by the end of 2024, to guard against instances of identity fraud. This is especially relevant to receive accounts being set up to receive scammed payments.

After seeking an appropriate authorisation from the ACCC, other sectors could similarly undertake an industry-wide process to identify equivalent technology measures that improve on existing identity verification and trust measures (while being alive to protection and promotion of individual privacy rights).

### Reducing exposure to scams

It is an unfortunate reality that "scam pollution" is pervasive, making it vital for the ecosystem's frontline protections to be bolstered – otherwise there will be overreliance on last line defences, acting "at the bottom of the cliff".

[3] https://www.ausbanking.org.au/new-scam-safe-accord/

Some of the most challenging scams for banks to disrupt involve consumers who have been exposed to sustained periods of social engineering (e.g. romance or investment scams), which, if successful, are typically lucrative for the scammer but life-altering for those impacted.

Westpac's internal "conversion rate" keeps track of instances where the bank has attempted to warn a customer (typically through a direct phone conversation) that a payment they are about to make could be a scam. Unfortunately, it is not always possible for the bank to achieve detachment from the scammer at this late stage – often after months of social engineering by the scammer – and the customer chooses to proceed with the payment despite being warned by the bank (even when the customer undertakes not to make the payment during the phone conversation).

It would be a far more effective protection for the customer to have never received the call or fake advertisement to begin with, or to have known the real identity of the person making the phone call or placing the digital advertisement.

When a person receives a text message or a phone call, they should have confirmation of who is texting or calling. When a person is considering an investment via a website, social media, or digital advertisement, they should have confirmation they are dealing with a legitimate entity. In short, the concept of confirmation of payee should be expanded across the ecosystem to improve confirmation of caller, confirmation of texter, and confirmation of an advertiser.

It is imperative the ecosystem works together to put Australians back in control of their own phones and computers (which are almost always the front door for scams), just as banks are investing in the payments system through confirmation of payee technology.

***Figure 2: The areas of uplift Westpac thinks could be considered to lift ecosystem-wide scam protections***

| Telecommunications Providers | Digital Platforms | Banks |
|---|---|---|
| • Track and report not just blocked calls, but also the number of scam messages and calls delivered – which will be a better metric for measuring scam harm. | • Introduce reporting and record keeping requirements – essential for customers to be able "prove" a link to a scams event (most won't keep copies of a digital ad; some won't remember which platform facilitated an interaction). | • Join the industry-established Australian Financial Crimes Exchange (AFCX) and receive and utilise AFCX data to fight scams. |
| • Introduce "anti-venom" obligations to alert a customer if known that a scam message/call has been delivered so prompt action can be taken to avoid the person being scammed. | • Introduce "anti-venom" obligations (the requirement to alert a user when a known scam advertisement has been interacted with). | • Implement processes to enable payee verification to reduce payments to scam accounts. |

| | | |
|---|---|---|
| • Review the rationale that allows for call spoofing – consumer protection benefits should outweigh any business justification. | • Recalibrate existing risk-settings to catch and block more scam content, increasing the tolerance for false-positive results/and need for additional internal content review. | • Increase warnings and use of payment delays by giving customers appropriate warnings when a customer is adding a new payee, amending a payee and increasing payment limits, and use technology to introduce risk-based delays. |
| • Introduce "one-click" reporting of suspected scam SMS or scam calls to telcos with a requirement to act on the information. | • Introduce "one-click" reporting of suspected scam content along with a requirement to act on the information. | • Make risk-based decisions about limiting high risk exit channels for the proceeds of scams (such as blocking, where appropriate, payments to some crypto exchanges). |
| • Have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). | • Have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). | • Have processes in place to identify consumers at a higher risk of being targeted by scammers (vulnerable cohorts). |
| • Mandatory participation in Government's SMS Sender ID registry. | • Where a known brand or identity is being used in an advertisement, take steps to confirm directly with that business/identity purportedly publishing the advertising content. | • Take steps to prevent misuse of bank accounts via identity fraud, such as through the use of biometric checks when new individual customers open new accounts online. |

**Introducing a "freeze switch" for accounts**

Westpac supports a requirement for banks to make available user-friendly and accessible methods for consumers to act immediately, should they suspect they have been scammed. However, further consideration is required to assess how an in-app "freeze switch" for accounts would assist with scam protection (noting scams are facilitated when a customer has themselves performed a transaction/action). For instances of fraud (typically involving an unauthorised transaction), Westpac customers have the existing in-app ability to action a card block or set their existing daily payment limit to zero.

Westpac is happy to consult further with Treasury directly on how best to deliver on this proposal's stated objective of making available methods for consumers to immediately act, should they suspect they have been scammed. We agree with the policy intent, but we believe the approach to address it requires further consideration to achieve the stated goal, and avoid

ineffective investment and outcomes, as well as unintended account blocking consequences which may exacerbate existing customer vulnerability (e.g. any missed recurring, direct debit or PayTo payments may impact a customer's access to essential services and result in 'missed payment fees' imposed by merchants).

It should also be noted that we have existing plans to increase our customer-oriented digital scam protections at the "front end" of the payment process. This includes enhancing our "Westpac Verify" feature and introducing dynamic in-app questioning in instances where a payment is considered a higher risk of being a scam[4].

## Recommendation 4:

*Accelerate the delivery of Government's SMS Sender ID Registry.*

Westpac recommends an accelerated timetable for implementation of the Government's SMS Sender ID Registry to deal effectively with the scourge of impersonation scams. It is presently possible for scammers to infiltrate legitimate text message exchanges between businesses and their customers, making it a far harder task for consumers to recognise a non-genuine communication.

According to the ACCC, in 2022 Scamwatch received 14,603 reports about bank impersonations with more than $20 million reported lost. More than 90 of these reports individually lost between $40,000 and $800,000[5]. Text messages were the leading contact method for scams in 2022, surpassing phone calls.

As the ACCC notes, this scam type is convincing when the scammer uses a spoofed phone number or alpha tag of the bank or other legitimate organisation. For this reason, Government's SMS Sender ID should also cover phone numbers, as opposed to just alpha tags.

Westpac has taken steps to effectively prevent call-based Westpac spoofing by working with our telco provider to enable 'Do Not Originate' technology for our ~94,000 registered phone numbers. While this has been effective in stopping call-based impersonations, there are limitations with extending this technology to text messages as our primary telco provider does not have alpha-blocking enabled and we use multiple providers to deliver SMS communications. Without a mandatory Sender ID Registry, such blocking is therefore limited and not guaranteed.

Westpac notes that pilot work on the SMS Sender ID Registry concept has commenced. It is our intention to join and support the pilot, however, we believe the proposed timeline for the register to be fully operational needs to be fast-tracked.

## Recommendation 5:

*Bring crypto exchanges and online marketplaces into the ecosystem immediately.*

Westpac believes a staggered approach to ecosystem implementation will result in sub-optimal outcomes for consumers, encouraging scammers to target industries that remain outside of the regulatory framework.

For this reason, crypto exchanges should enter the ecosystem at or about the same time as the other identified sectors (banks, telecommunications providers, and digital platforms).

[4] https://www.westpac.com.au/about-westpac/media/media-releases/2023/31-August/
[5] https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf

Recent analysis of data undertaken by the AFCX found that 47 per cent of scam funds were directed to accounts associated with cryptocurrency exchanges in the last 30 days of the last financial year[6], with funds moving offshore and irrecoverable. Closing the exit channel for scam funds is imperative to the integrity of our ecosystem.

While some banks, including Westpac, have begun blocking payments to certain crypto exchange platforms that pose an unacceptable level of risk, a key issue remains that once scam funds are transferred into crypto, they can be virtually impossible to recover.

Similarly, exclusion of online marketplaces from the initial ecosystem appears to be an oversight given the role they play as a prevalent transmission channel for buying and selling scams.

While it is difficult from a banking perspective to determine whether a payment someone is about to make is for a genuinely offered good advertised on a marketplace, conversely the ACCC's Digital Platform Services Inquiry's fourth interim report found that "online marketplaces have a high level of control and involvement in transactions between consumers and sellers on their platforms."[7] An investigation undertaken overseas by UK bank TSB's fraud team recently found that more than one third of one particular platform's marketplace ads could be scams[8]. Scammers target people both seeking to buy and sell their goods on online marketplaces.

## Recommendation 6:

*Use a pragmatic but flexible definition of scams, which for the banking sector, draws a distinct line between scam and fraud activity.*

Westpac has concerns about the proposed definition of scams set out in the Consultation Paper, given it erodes the essential distinction between a fraud and scam event. Using a definition in the criminal code that attracts criminal penalty and applying it to a civil penalty regime requires more careful consideration of consequential impact.

While the word "scam" is often synonymous with "fraud" in general usage, in banking "scam" and "fraud" have distinctly separate meanings. The defining difference between a fraud and scam event is typically "customer authorisation". A scam involves a transaction/action that was performed by the customer, whereas fraud occurs when the customer was not involved in performing the transaction.

To ensure consistency of approach, we note the ePayments Code already has clear definitional delineations between frauds and scams. We further note that Treasury is already tasked with reviewing the scope and applicability of the ePayments Code as part of its ongoing Payments System Reform review. Definitional consistency is critical, and therefore we ask that the ePayments Code review is undertaken to ensure interoperability with development of the Scams Code Framework.

[6] https://www.afcx.com.au/2023/08/14/half-of-all-scam-funds-flow-to-cryptocurrency/
[7] https://www.accc.gov.au/media-release/concerning-issues-for-consumers-and-sellers-on-online-marketplaces#:~:text=The%20ACCC's%20fourth%20report%20in,and%20sellers%20on%20their%20platforms
[8] https://www.tsb.co.uk/news-releases/urgent-consumer-warning-as-tsb-finds-over-a-third-of-adverts-on-facebook-marketplace-could-be-scams

## Appendix 1: Examples of Westpac's scam protection measures

| | |
|---|---|
| **Westpac Verify** | Customers are alerted to a potential account name mismatch for first-time transfers to a new payee, or where money is being sent to an account Westpac has never transacted with before, for payments made via the New Payments Platform. Payments are paused for four hours so customers have an opportunity to check if payment details are correct. |
| **Enhanced Westpac Verify** | When customers enter a new payee into their online or mobile banking for the first time, they will be presented with a scam risk assessment to help customers determine whether they want to proceed with a payment. This includes when there is a potential account name mismatch to a new BSB and account number or when money is being sent to an account a Westpac customer has never transacted with before. Commencing in 2024. |
| **New payment prompts** | Set to roll out in 2024, customers will be presented with a series of dynamic questions in instances where a payment is considered a higher risk of being a scam. The prompts will be activated if Westpac's fraud systems detect a potential scam after payment details are entered into their online or mobile banking. If Westpac still considers the payment is highly likely to be a scam risk based on the information provided, the payment will not be allowed to be processed. |
| **Scam blocks** | Real-time blocking of suspect online merchants, with over $131 million saved for 1.54 million scam customers since January 2022. |
| **Stopping spoofing calls** | Westpac has worked with our telecommunication provider Optus to add 94,000 Westpac numbers to the 'Do Not Originate' list, preventing scammers from impersonating the bank's phone numbers. |
| **Sophisticated detection technology** | Advanced customer behavioural tool launched in mid-2022 to help combat remote access, saving over $13 million for customers to date. |
| **Crypto exchange blocks** | New customer protection blocks for some cryptocurrency payments to reduce scam losses. |
| **Dedicated Financial Crime Hub** | Recently opened in Parramatta Square, NSW bringing over 500 scam, fraud & financial crime specialists together. |
| **Implementation of the ABA's Scam-Safe Accord** | Westpac has committed to a comprehensive set of anti-scam measures, set out at: www.ausbanking.org.au/new-scam-safe-accord/ |
| **Scam education & awareness** | Ongoing scam awareness warnings/alerts delivered directly to customers in online and mobile banking, as well as education campaigns and seminars for customers. |