SCAMS PREVENTION FRAMEWORK AND AML/CTF REFORMS

COORDINATING YOUR APPROACH

Contents

Scams and AML/CTF – two reforms that go hand in hand

Two significant pieces of regulatory reform have been enacted by the Federal government with the passage of:

- the *Scams Prevention Framework Bill 2025*, to amend the *Competition and Consumer Act 2010* (Cth) (**CCA**) in February 2025; and
- the *Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024* (**Amendment AML/CTF Act**), to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) in December 2024.

These two separate regulatory reforms have their own scope, regulators, obligations and start date. But they also have a lot in common. Given the significant intersection between the regimes, banks should be approaching the reforms with a coordinated approach.

In this article we have considered key aspects of the Scams Prevention Framework (**SPF**) and how this relates to anti-money laundering and counter-terrorism financing (**AML/CTF**) developments for the banking sector.

What is the Scams Prevention Framework?

Overview of the SPF

The SPF has been enacted as a framework for preventing and responding to scams. The regime establishes principles which regulated entities must follow in connection with:

- their governance arrangements for combatting scams; and
- preventing, detecting, reporting, disrupting and responding to scams.

Application of the SPF regime

What amounts to a scam?

The purpose of the SPF is to prevent and respond to scams. What is a scam?

The SPF defines a scam broadly as:

"a direct or indirect attempt (whether or not successful) to engage an SPF consumer of a regulated service where it would be reasonable to conclude that the attempt:

(a) involves deception (see subsection (2)); and

(b) would, if successful, cause loss or harm including obtaining SPF personal information of, or a financial or other benefit from, the SPF consumer or the SPF consumer's associates."

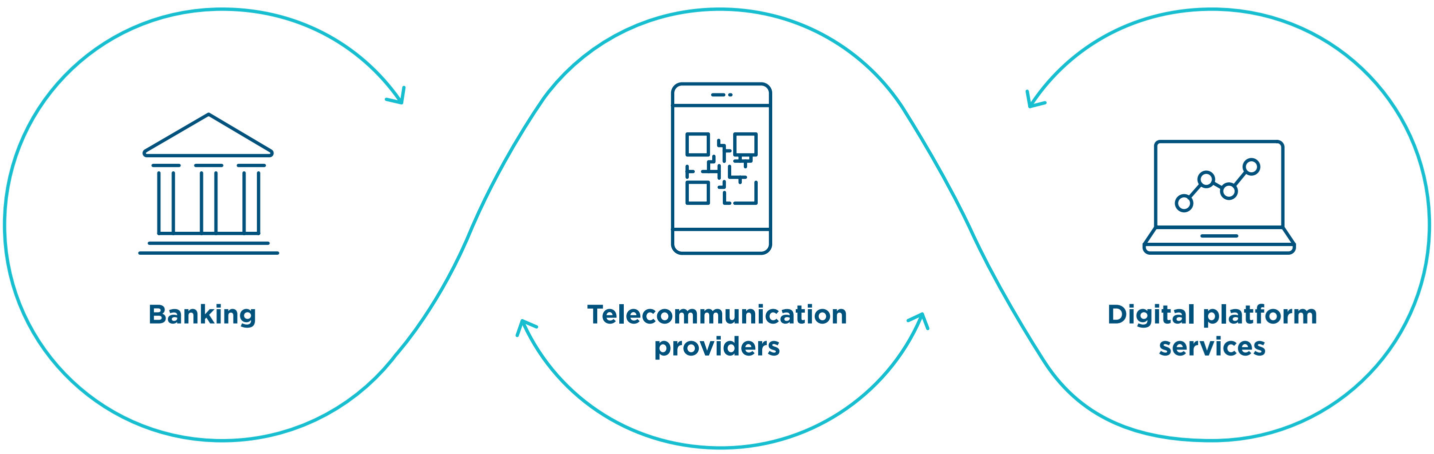
There are several aspects to the definition. However, as an overarching statement, the definition of scam is deliberately broad and is intended to capture a range of activity including remote access scams, phishing scams, investment scams and a raft of others. Given its breadth it is also possible that certain conduct that is not ordinarily thought of as a "scam" may fall within the definition, such as when a customer's bank account is used as part of a cuckoo smurfing operation.

It is likely that certain incidents will be excluded from the definition of scams once the rules are made to accompany the regime. The Explanatory Memorandum to the legislation introducing the SPF provides some examples of potential exclusions from the definition of scam, such as certain subsets of fraud, cybercrime, and misleading or deceptive conduct in trade or commerce.

What entities are regulated under the regime?

The SPF will only apply to a "regulated entity". This concept is contingent on the entity being part of a "regulated sector". A regulated sector must be designated by the Minister. It is also possible that specific businesses or services could be designated.

No designations have been made to date. However, the expectation is that the following three sectors will be the first to be designated:



Providers of services within these sectors are therefore particularly focussed on the impact of the SPF and preparing for its commencement.

The SPF is not a reimbursement regime

The SPF sets out principles that reporting entities must comply with and civil penalties attach to failures to comply with those principles. While the SPF is not a consumer compensation scheme, it does give consumers the right to bring a claim in Court to seek to recover loss or damage suffered because of the conduct of another person in contravention of civil penalty provisions under the SPF.

Current status of the SPF

The SPF will not take effect until a sector is designated under the regime.

There are a range of other practical questions that will need to be worked through as the SPF regime develops and the Rules and Codes are consulted on. Such questions include:

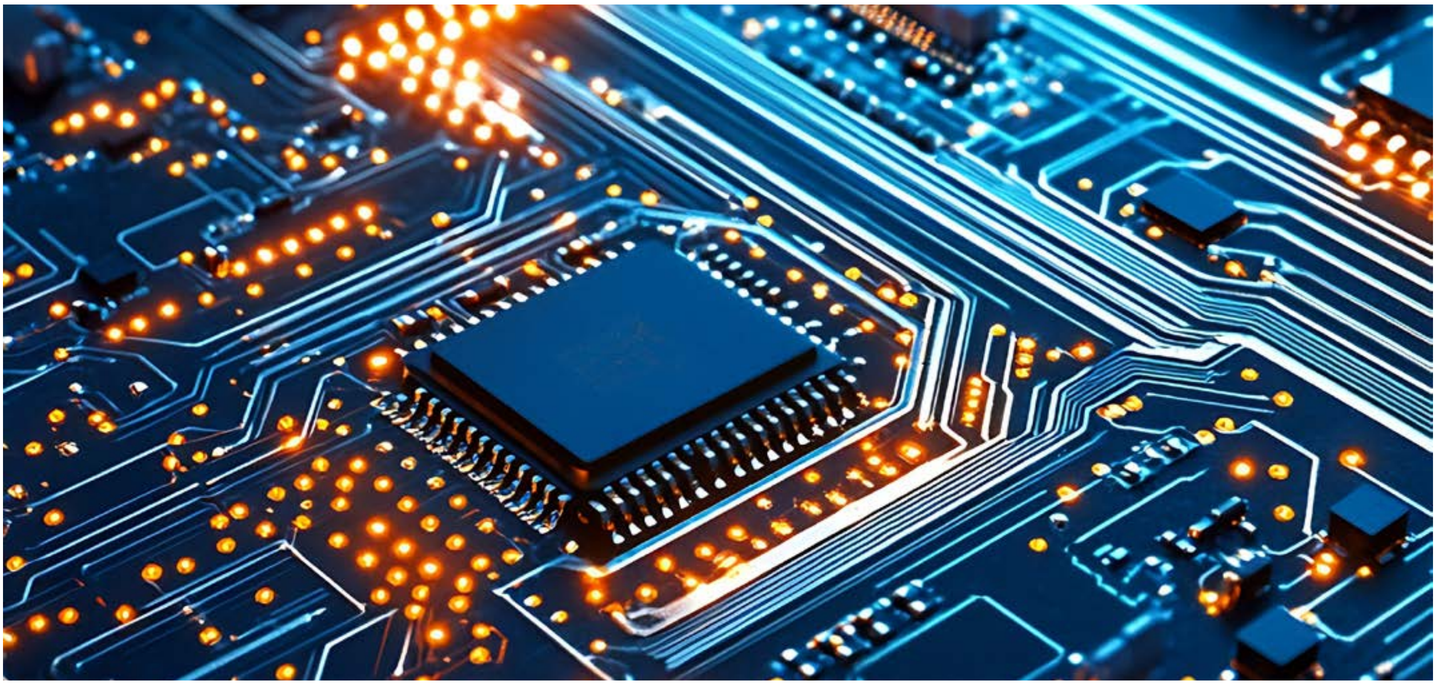
- How internal dispute resolution mechanisms will manage complaints where the complaint comes to one regulated entity but there are other regulated entities in the chain of events that led to the scam – for example, a scam is advertised in a digital platform or a customer receives a promotional text message and makes a payment through their bank account.
- How will existing regulatory regimes and liability frameworks operate? For example, what will the role of the ePayments Code be going forward?
- How will AFCA prepare for their expanded remit and managing the handling of complaints involving multiple regulated entities from outside the financial services sector?
- How will the SPF Codes develop the concept of "reasonable steps" and what should reporting entities be doing now to prepare for these expectations?

While there are a range of topics that require deep engagement, for the purpose of this article we have focussed on aspects of the SPF regime that intersect with AML/CTF requirements.

Legislation in development

While the amendments to the CCA have been enacted, there is a significant amount of detail that is left to be set out in the supporting:

- SPF Rules; and
- SPF Codes.



Reporting under the SPF and AML/CTF regime

SPF: Reporting actionable scam intelligence to the ACCC

SPF principle 4 is "**Report**" – sharing information has been identified as a key step to meet the object of the SPF. The intention is that sharing information should allow other reporting entities and regulators to respond accordingly.

As part of this principle, regulated entities must report to the ACCC where they have "actionable scam intelligence". This means that a bank will need to report to the ACCC, within a period to be prescribed, if:

"there are reasonable grounds for the entity to suspect that a communication, transaction or other activity relating to, connected with, or using a regulated service of the bank is a scam."

AML/CTF: Reporting suspicious matters to AUSTRAC

Reporting to AUSTRAC is a fundamental aspect of the AML/CTF regime.

Entities regulated under the AML/CTF Act are referred to as "reporting entities" for a reason – they are charged with acting as the eyes and ears of Australia's financial intelligence unit and sharing relevant information that they identify in the provision of services.

Reporting entities are required to report a range of matters to AUSTRAC. This includes where the reporting entity:

- suspects, on reasonable grounds, that a customer isn't who they claim to be; or
- suspects, on reasonable grounds, that they may have information that is relevant to the investigation of, or prosecution of an offence.

When a prescribed suspicion arises, the reporting entity must make a suspicious matter report (**SMR**) to AUSTRAC within prescribed periods.

Eyes and ears"

Reporting entities are the eyes and ears of Australia's financial intelligence unit because of the information they identify and share to AUSTRAC in the provision of their services.

The intersection of SPF and SMR reporting requirements

It is easy to imagine how an obligation to report actionable scam intelligence could also require a SMR to be lodged. For example, the following scenarios are likely to amount to actionable scam intelligence that must be reported to the ACCC and will also require an SMR to be filed with AUSTRAC:

- there is a suspicion that a customer has been using fraudulent information in setting up an account with a bank for the purpose of scam connected activity; or
- there is a suspicion that an account is being used to receive payments connected to scam activity.

The need to report actionable scam intelligence to the ACCC could easily be viewed as another new process that banks need to create. However, in establishing a framework for reporting actionable scam intelligence to the ACCC, banks should leverage the existing transaction monitoring and SMR process that is currently in place for AML/CTF purposes.

Associated SMR and SPF reporting

While it will need to be uplifted for the SPF, in our view it is appropriate for the SPF reporting regime to operate hand in hand with AML/CTF SMR process.

What happens after a report is made?

SPF: Investigating and disrupting potential scam activity

SPF principle 3 is "**Detect**" – this includes the ongoing obligation to take reasonable steps to detect scams, including investigating activities subject of actionable scam intelligence.

SPF principle 4 is "**Disrupt**" – if an activity is suspected of being a scam, the regulated entity must take reasonable steps to disrupt it.

Under the SPF, the obligations of a bank don't stop once the actionable scam intelligence has been reported to the ACCC. The bank has 28 days to take reasonable steps to investigate whether the activity is a scam. It is also contemplated that the outcome of that investigation will need to be reported to the ACCC.

The bank will also be required to take reasonable steps, within a reasonable time, to disrupt the activity or prevent loss or harm (including further loss or harm) arising from the activity. At this stage, it is unclear what steps will be considered 'reasonable' but we expect that what is appropriate will vary between regulated entities.

What do reasonable steps to investigate involve?

What is a reasonable to disrupt and prevent loss and harm?

How much engagement will this involve from customers?

AML/CTF: What is required after lodging an SMR?

Under both the current and Amended AML/CTF Act, making a SMR would typically result in a reporting entity considering the ongoing risk associated with the customer relationship, making a decision in connection with enhanced due diligence and the appetite to continue the customer relationship.

SMR obligations are being updated as part of the AML/CTF reforms. This includes proposed updates to the expectations on transaction monitoring for identifying suspicious matters. The Draft Rules also contemplate the introduction of requirements in connection with the timely review and determination of matters that are potentially suspicious.

The updated ongoing due diligence measures introduced in the Amended AML/CTF Act will prescribe that the reporting entity must review and, where appropriate, update the identification of ML/TF risk associated with the customer if there are behaviours that give rise to a SMR obligation. The reporting entity will also be required to apply enhanced CDD to the relationship.

Be wary of tipping off

The reporting entity will need to be mindful of the tipping off offence. While recently updated to be more adaptable to modern business structures, tipping off remains a criminal offence and can be committed by both the reporting entity and individuals within the entity.

WHAT HAPPENS AFTER A REPORT IS MADE?

Investigating and disrupting under SPF while managing ML/TF risk and tipping off

Managing the customer relationship

Both the SPF and the AML/CTF regime require a bank to engage in further steps after making a report. The process to investigate and disrupt potential scam activity should be designed having regard to the measures required under the AML/CTF Act. For example:

Investigation	When investigating whether there is a scam, the bank may ask customers clarifying details. Any information that is obtained as part of this "detection" step should be considered as part of the information that the bank holds in connection with its customer and the assessment of ML/TF risk. If information is collected as part of the scams investigation process, this should not be siloed and may be an important part of the ongoing due diligence on the customer under the AML/CTF.
Decision making	When deciding to disrupt activity, such as blocking accounts or halting trades, the bank will need to carefully manage communications with customers to ensure that the tipping off offence is not triggered. While the offence has been updated and can operate in a more practical way, it remains something to be taken seriously and managed as part of customer engagements.

Engaging with other reporting entities

As part of the tipping off reforms, an express exemption has been added to the disclosure of information between reporting entities where the disclosure is made for the purpose of detecting, deterring, or disrupting money laundering, the financing of terrorism, proliferation financing (**ML/TF/PF**), or other serious crimes.

However, the exclusion only applies if conditions prescribed by the regulations are met. No conditions have been prescribed by the regulations to date. In AUSTRAC's guidance on tipping off, AUSTRAC is of the view that the exemption is not available until regulations are made to prescribe conditions.

It is anticipated that Regulations will establish a framework to enable private-to-private sharing of information which would be subject to appropriate controls and safeguards yet to be prescribed. A similar regime is being introduced in Hong Kong through a platform to be rolled out by the Hong Kong Monetary Authority.

However, in Australia, while we wait for such a framework to be developed, this does not mean that information sharing between reporting entities for the purpose of detecting, deterring, or disrupting ML/TF/PF, or other serious crimes will always be tipping off. However, if the disclosure:

- does not disclose information covered by the tipping off offence; and/or
- would not or could not reasonably be expected to prejudice a prescribed investigation,

then the tipping off offence is not triggered, irrespective of the availability of exemptions.

Therefore, while this type of information sharing may be useful for ML/TF/PF and serious crime prevention more generally, it should also be considered as part of bank's implementation of information sharing arrangements in connection with scams, whether under the SPF once enacted or otherwise.

Governance expectations – regulatory super theme

Governance and SPF

Overarching the SPF is an obligation to have documented governance arrangements to combat scams. This is reflected in SPF principle 1: "**Governance**".

The SPF requires regulated entities to:

1

Document polices

Document policies and procedures about:

- preventing, detecting and disrupting scams;
- responding to scams; and
- reports related to scams.

2

Implement polices

Implement the developed governance policies and procedures.

3

Document targets

Develop and implement performance metrics and targets for measuring the effectiveness of those governance policies and procedures.

As well as the maintenance and implementation of the policies, procedures and metrics, a senior officer must make an annual certification about compliance with these governance arrangements. The senior officer is a person that is an officer or senior manager within the meaning of the Corporations Act.

AML/CTF and governance - a continued focus

Governance connected to AML/CTF compliance arrangements continues to be a key focus of AUSTRAC and is developed as part of the AML/CTF reforms. This includes embedding the responsibility of the governing body of a reporting entity into the AML/CTF Act.

As part of the changes, a new role of "senior manager" is introduced into the AML/CTF framework. The role of senior manager will have a number of responsibilities including:

- approving the AML/CTF policies and ML/TF risk assessment of the reporting entity, and updates to these; and
- under the Draft Rules, giving approval to certain relationships including relationships with foreign and high risk PEPs and nested service relationships.

GOVERNANCE EXPECTATIONS – REGULATORY SUPER THEME

Intersection between SPF and AML/CTF governance requirements

"Governance" is a regulatory super topic – it is a consistent focus of regulators and is becoming more embedded into statutory frameworks. The SPF is no different and the trend continues with updates to the governance expectations connected to AML/CTF.

For example, both the SPF and AML/CTF reforms use similar concepts in the role of "senior officer" under the SPF and "senior manager" under the AML/CTF regime:

Senior officer under SPF	Senior manager under AML/CTF
Officer under the Corporations Act: This includes a prescribed roles including director or secretary of a corporation and also includes a person who: • who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the corporation; or • who has the capacity to affect significantly the corporation's financial standing; or • in accordance with whose instructions or wishes the directors of the corporation are accustomed to act (excluding advice given by the person in the proper performance of functions attaching to the person's professional capacity or their business relationship with the directors or the corporation). **Senior manager** under the Corporations Act: In relation to a corporation, means a person other than a director or secretary who: • makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the corporation; or • has the capacity to affect significantly the corporation's financial standing.	An individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the reporting entity.

In implementing both the SPF and the AML/CTF updates, regulated entities will need to consider the appropriate person or persons to fulfil the above roles under each regulatory regime. Whether or not one person sits in the prescribed positions across the SPF and AML/CTF, the individual(s) that are appointed under each regime will need have an appropriate understanding of their roles and responsibilities.

Identifying and appointing the relevant persons is likely to require internal discussion and consideration and time to ensure that the person(s) is on board with their role and understands their responsibilities.

Planning for the new regimes

The AML/CTF updates and the new SPF regime are waiting on further detail about how these updates will operate in practice. At this stage, the AML/CTF Rules are not finalised and AUSTRAC is yet to issue guidance in connection with the new regime. In addition, the SPF is also to be supported by Rules and Codes that have not been released. Accordingly, while it may seem appropriate to wait until these aspects of the changes are settled, we expect that the implementation of these regimes will require swift action. Regulated entities should be thinking now about their current frameworks and should ensure that any projects on one regulatory reform connects with the other.

Contacts

Alice Molan
Partner
T +61 3 9288 1700
alice.molan@hsf.com

Daniel Hyde
Senior Associate
T +61 2 9225 5480
daniel.hyde@hsf.com

Julia Massarin
Special Counsel
T +61 3 9288 1117
julia.massarin@hsf.com

Bryony Adams
Partner
T +61 2 9225 5288
bryony.adams@hsf.com

Andrew Eastwood
Partner
T +61 2 9225 5442
andrew.eastwood@hsf.com

Felix Hu
Senior Associate
T +61 2 9225 5664
felix.hu@hsf.com

Kate Cahill
Partner
T +61 2 9322 4413
kate.s.cahill@hsf.com

Charlotte Henry
Partner
T +61 2 9225 5733
charlotte.henry@hsf.com

Tess Meaden
Solicitor
T +61 3 9288 1215
tess.meaden@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**