Paul Melling & Associates Pty Limited

Breach (Reportable Situation) and Events Reporting Policy

This policy applies from 1 October 2021.

Document Control:	Version 2
Last reviewed by:	Steve Melling on 13th September 2021

At a glance

Responsibility, review and breaches of this policy

The Compliance Manager is the "Responsible Person" who oversees this policy. For this current document the Compliance Manager is Steve Melling.

The policy is reviewed periodically in accordance with our Compliance Diary & Checklist.

Identify
- As an AFS licensee, we must ensure that our representatives (including employees, officers and agents) are aware of their obligation to identify and escalate any reportable situations, incidents, breaches and likely breaches.

Assess
- All reportable situations, incidents, breaches and likely breaches must be promptly assessed in accordance with the relevant provisions of the law, as set out in this policy. The assessment should also be properly documented in the Breaches and Incidents Register.

Report
- Reportable situations must be reported to ASIC as soon as practicable, and, in any event, within 30 days, as described in this policy.

Rectify
- Rectification is just as important as reporting. This requires us to take reasonable steps to prevent the situation from happening again. Depending on the circumstances, this requires us to notify clients, other licensees, and investigate and remediate within specified timelines

Why does this policy matter?

We all need to follow this policy because it helps us to meet our legal obligations and stay within our risk appetite.

Key requirements

Licensee

Do	When
Where you are aware of a reportable situation, incident, breach or likely breach, report it to your Compliance Manager	Immediately
 Record all reportable situations, incidents, breaches and likely breaches in our Breach Register	As soon as the reportable situation, incident, breach or likely breach has been assessed in accordance with the requirements set out in this policy
Notify ASIC of reportable situations	Within 30 days, in accordance with the requirements set out in this policy
Provide representatives with adequate training about this policy.	At least annually
Notify ASIC of other events	 Within the prescribed timeframe for each event – see the Reporting Table referred to later in this policy

Representative

Do	When
Where you become aware of a reportable situation, incident, breach or likely breach, report it to your licensee	Immediately
Attend adequate training that covers off on identifying, assessing and reporting those reportable situations, incidents, breaches or likely breaches	At least annually

DO NOT	
Fail to report breaches, likely breaches, incidents, or reportable situations internally for assessment	
Deem breaches to be not reportable, where they should in fact be reported	
Fail to notify ASIC of other events set out in the Reporting Table	 Within the prescribed timeframe for each event in the Reporting Table

Introduction and scope

An AFS licensee has an obligation to notify ASIC of certain types of events and breaches of the law.

This policy contains two sections:

- **Notifying ASIC of reportable situations**

  This involves identifying, assessing, reporting and rectifying incidents, likely breaches and breaches internally, as well as lodging a report with ASIC, for reportable situations we identify; and

- **Notifying ASIC of other events**

  This involves reporting other necessary information (e.g. change of business address) to ASIC.

Notifying ASIC of reportable situations

This policy is separate and in addition to any breach reporting policies imposed on us by any laws other than the Act, other licensees, or principals under any binder or other agreement.

See “Step 1” below for an explanation of what is a reportable situation.

Training and communication

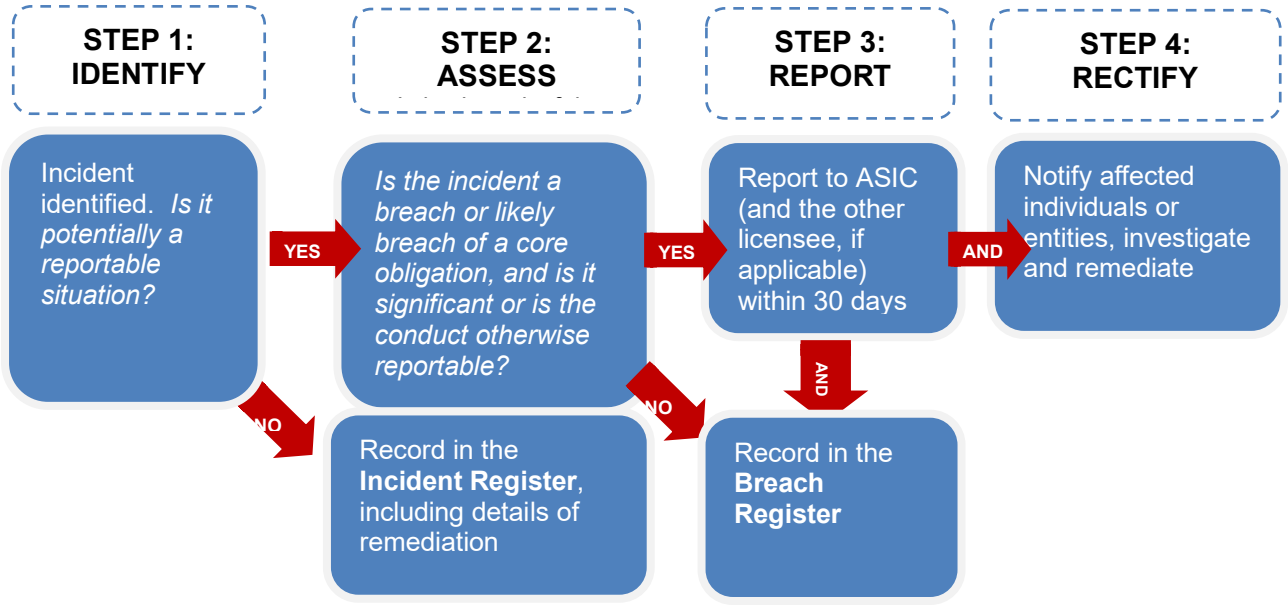
All staff are trained in compliance obligations and are required to report any breach of our policies and procedures, or any suspected breach of the core obligations, to the Compliance Manager. The Responsible Person ensures that training takes place.

The Compliance Manager will meet with representatives if they believe incidents, breaches, likely breaches or other reportable situations may have arisen. If any staff member becomes aware of a breach or likely significant breach of the core obligations, or another reportable situation, they must immediately discuss it with the Compliance Manager who will complete the Breaches and Incidents Register, which includes a breach assessment tool and a draft report feature.

Paul Melling & Associates and all its representatives understand that failing to report a significant breach of the core obligations, or other reportable situation to ASIC, within 30 days after we first know, or are reckless with respect to whether there are reasonable grounds to believe, the situation has arisen, constitutes a separate breach of Paul Melling & Associates Pty Limited’s licence and the Act.

The reporting process – a summary

The Compliance Manager ensures that breaches and incidents are identified and recorded and that reportable situation notices are lodged with ASIC, by following the process illustrated below.



STEP 1 IDENTIFY: AN INCIDENT HAS BEEN DISCOVERED. IS IT POTENTIALLY A REPORTABLE SITUATION? IF IT IS, GO TO STEP 2.

An incident is an action or failure to act that is a breach of law or our policy. Ask questions:

a. Has something gone wrong?

b. Has a policy been breached?

c. Have we done something that's potentially misleading?

d. Has the licensee or a representative potentially done something illegal?

e. Do you suspect that a reportable situation has occurred but you're not sure?

If yes, an incident may have occurred, and you must tell the Compliance Manager immediately.

The incident must be assessed and reported, where required, within 30 days. The Compliance Manager ensures that it is recorded in the appropriate register.

STEP 2 ASSESS: ASSESS THE INCIDENT TO SEE IF IT'S A BREACH OR A REPORTABLE SITUATION. IF IT IS, GO TO STEP 3.

It is the responsibility of the Compliance Manager to record all incidents in the Incident Register, and all breaches, likely breaches and reportable situations, in the Breach Register.

It is also the responsibility of The Compliance Manager to record and file all correspondence and information which relates to a breach.

If the breach is a significant breach (or likely to be a significant breach), or constitutes a reportable situation for any other reason, then proceed to Step 3.

What is a reportable situation?

A reportable situation[1] occurs if a financial services licensee or their representative:

1. Breaches, or likely breaches, a core obligation, and the breach is significant. Some breaches are *deemed* significant.	**Significant breach**
2. Investigates (1) and if the investigation continues for more than 30 days. Even if no reportable situation is identified, the investigation itself is a reportable situation if it continues for more than 30 days.	**30+ day investigations**
3. Engages in gross negligence or commits serious fraud.	**Gross negligence or serious fraud**
4. Believes[2] that another individual has engaged in conduct (1) or (3) above, and they're another licensee or a representative of another licensee who provides personal advice to retail clients in relevant financial products.	**Other licensees and their adviser's conduct**

Sometimes, our representatives report issues which may not constitute a reportable situation, but are still a breach of our statutory obligations, policies or processes. Unless or until the breach is found to be a breach of the core obligations, the issue is called an "incident". The Compliance Manager will determine whether or not an incident amounts to a breach of the core obligations, or is a reportable situation, for any other reason. They may seek external legal assistance in making this determination.

1. Significant Breach: Is it a breach or likely breach of a core obligation that is significant? If yes, go to Step 3. If no, record it in the Incident Register.

a. What is a breach or likely breach?

A *breach* is a contravention of a core obligation by us or our representatives. A *likely breach* occurs when we or our representatives are no longer able to comply with a core obligation.

b. What is a core obligation?

Section 912D of the Act applies to breaches of core obligations which include the requirement to:

- do all things necessary to ensure that the financial services covered by our AFSL are provided efficiently, honestly and fairly;
- comply with the conditions on our licence;
- manage conflicts of interest;
- have adequate resources to provide the financial services covered by our licence and to carry out supervisory arrangements;
- be competent to provide the financial services covered by our licence;
- have trained and competent representatives;
- take reasonable steps to ensure that our representatives comply with the financial services laws;
- have a dispute resolution system for retail clients;
- have adequate risk management systems;[3]
- have compensation arrangements for retail clients;[4] and
- comply with certain financial services laws[5]. The relevant financial services laws are:
    - Chapter 5C of the Act (managed investment schemes);
    - Chapter 5D of the Act (licensed trustee companies);

- Chapter 6 of the Act (takeovers);
- Chapter 6A of the Act (compulsory acquisitions and buy-outs);
- Chapter 6B of the Act (rights and liabilities in relation to Chapters 6 and 6A matters);
- Chapter 6C of the Act (information about ownership of listed companies and managed investment schemes);
- Chapter 6D of the Act (fundraising);
- Chapter 7 of the Act (financial services and markets);
- Chapter 9 of the Act (miscellaneous), but only as it applies in relation to the Chapters of the Act listed above;
- Division 2 of Part 2 of the *ASIC Act 2001* (unconscionable conduct and consumer protections in relation to financial services); and
- other Commonwealth legislation specified in the regulations, in so far as they cover conduct relating to the provision of financial services. These are:
    - *Financial Sector (Collection of Data) Act 2001*
    - *Insurance Acquisitions and Takeovers Act 1991*
    - *Insurance Act 1973*
    - *Insurance Contracts Act 1984*
    - *Life Insurance Act 1995*
    - *Retirement Savings Accounts Act 1997*
    - *Superannuation Industry (Supervision) Act 1993*
    - *Superannuation (Resolution of Complaints) Act 1993*[6]

Breach of AFSL conditions: our AFSL conditions can be found at afsl.melling.com.au.

Only a breach or likely breach of a core obligation that is significant (or another reportable situation) is reportable. So, if we breach our obligations under, say, the Privacy Act, that is not a core obligation, and this regime doesn't apply. See, instead, our Data Breach Response Policy.

c. When is the breach or likely breach significant?

There are two ways that a breach or likely breach are significant:

(i) If the breach is *deemed* significant

Search the "Deemed significant breaches" tab in our Breaches & Incidents Register to search whether the breach is deemed significant. The breach or likely breach is *deemed* significant if it meets certain requirements – including:

- the breach is the commission of an offence under any law punishable by imprisonment for:
    - 3 months or more where the offence involves dishonesty; or,
    - 12 months or more in any other case;[7]
- there has been a breach of a civil penalty provision (most of the s912A obligations, including the efficiently, honestly and fairly obligation are civil penalty provisions). Other civil penalty provisions include breach of some directors' and officers' duties, and if the Licensee contravenes the best interests obligations[8] ;
- there has been a breach of the misleading and deceptive conduct provisions;
- the breach results in or is likely to result in, material loss or damage to members of superannuation entities or managed investment schemes or any person whether retail or wholesale who was provided with a financial service or product by Paul Melling & Associates Pty Limited or their representative.

- "Likely to result in" means that there is a real and not remote possibility that loss or damage will occur as a result of the breach.[9]
- "Material loss or damage" includes financial and non-financial loss or damage. 'Loss or damage' has its ordinary meaning, which is extensive. Whether a breach results or is likely to result in material loss or damage to a person will depend on the person's circumstances. For example, a relevant circumstance may include the person's financial situation. If a breach affects a number of people, it is sufficient for significance to be established if the breach is likely to result in material loss or damage to one person. Additionally, where the breach affects a number of people, licensees should consider the total loss or damage resulting from the breach. For example, even if the breach does not result in a material loss or damage to individual persons, the total loss or damage to persons resulting from the breach may, when aggregated, amount to material loss or damage to persons, thereby satisfying the significance requirement. Consistent with the common law position, 'likely to result in material loss or damage' is intended to mean that there is a real and not remote possibility that loss or damage will occur as a result of the breach.[10]

(ii) If the breach is not deemed significant under paragraph 1c(ii) above but is significant after considering 3 factors

If the breach or likely breach is not deemed significant, but it's still significant after considering:

- number or frequency of similar breaches;
- impact of the breach on our ability to provide financial services; and
- the extent to which the breach indicates that our arrangements to ensure compliance with our obligations are inadequate.

2. 30+ Day Investigations: Have we been investigating a significant breach or likely breach for more than 30 days? If yes, go to Step 3.

Have we been investigating, for more than 30 days whether a significant breach of a core obligation (for a description of "core obligations", see heading 1(b) above) has occurred, or whether the Licensee or a representative is no longer able to comply with a core obligation, and the breach, if it occurs, will be significant?

ASIC says that routine investigation (like an internal audit) that was not directed at identifying with a significant breach has arisen, does not constitute an investigation.[11]

If the incident involves such an investigation, proceed to Step 3.

3. Have we or our representative engaged in gross negligence or committed serious fraud? If yes, go to Step 3.

a. What is gross negligence?

Gross negligence does not have a precise meaning under Australian law. As a guide, gross negligence represents something more fundamental than failure to exercise proper skill and/or care, and with a disregard for obvious risks.

b. What is serious fraud

Serious fraud refers to an offence involving fraud or dishonesty against an Australian law or any other law, that is punishable by imprisonment for life or for a maximum period of at least three months. Falsifying documents is an example of serious fraud.

4. Do we believe that another individual has engaged in conduct (1) or (3) above, and they're another licensee (or a representative of another licensee) who provides personal advice to retail clients in relevant financial products? If yes, go to Step 3. :]

a. Conduct of other AFS licensees

Paul Melling & Associates Pty Limited must also lodge a report with ASIC if Paul Melling & Associates Pty Limited has reasonable grounds to believe that a reportable situation, other than a reportable situation about an investigation, has arisen in relation to an individual who:

- provides personal advice to retail clients about relevant financial products; and
- is any of the following:
    - another financial services licensee;
    - an employee of another financial services licensee (or a related body corporate of another licensee), acting within the scope of the employee's employment;
    - a director of another financial services licensee (or a related body corporate of another licensee), acting within the scope of the director's duties as director; or
    - a representative of another financial services licensee, acting within the scope of the representative's authority given by the licensee.

However, if there are reasonable grounds to believe that ASIC is aware of the reportable situation and all of the information that is required in a report, you don't need to lodge the report. ASIC says:

Note: For example, if you know that the other licensee or another third-party licensee has lodged a breach report with ASIC in relation to the reportable situation, you are not required to lodge a further report with ASIC.

b. Lodgement with ASIC

The report must be lodged with ASIC within 30 days after the reporting licensee first knows (or is reckless with respect to whether there are reasonable grounds to believe) that the reportable situation has arisen in relation to another licensee. See Step 3 below.

c. Informing the other AFS licensee

Paul Melling & Associates Pty Limited must also provide a copy of the report lodged with ASIC to the licensee who is the subject of that report. In some cases, this will require us to provide a copy of the report directly to the financial adviser if the adviser operates under their own financial services licence, or to a financial services licensee who is no longer involved with the financial adviser (for example, a previous employer). The report must be provided to the other AFS licensee within 30 days after we first know that, or are reckless with respect to whether, there are reasonable grounds to believe such a reportable situation has arisen. ASIC says:

For example, if a financial adviser who is the subject of your report operates under their own AFS licence, you must give a copy of the report directly to the financial adviser. If the financial adviser is a representative or employee of an AFS licensee, you should give a copy of the report to the licensee, even if that financial adviser is no longer involved with the licensee (e.g. previous employer).[12]

In providing the report to ASIC or the other licensee, we may have qualified privilege in an action for defamation if we had no malice.[13] We may also not be liable for an action based on breach of confidence in relation to the conduct.[14]

STEP 3 REPORT: REPORT TO ASIC

It is the responsibility of The Compliance Manager to lodge a report about reportable situations with ASIC, within 30 days after Paul Melling & Associates Pty Limited first knows (or is reckless with respect to whether there are reasonable grounds to believe), the situation has arisen. It is typically when the Compliance Manager is aware (or reckless to being aware) of the breach or reportable situation, that the 30 days begins – because they have actual authority to make a decision about lodging a breach report.

(Note: The 30 days may start if another person is aware and they have *apparent* authority in performing their role. See below, and ASIC's RG 78.73-81 for commentary and summaries of case law on this point).

The Compliance Manager will:

1. contact Paul Melling & Associates external compliance lawyers for advice (if it is decided that this is necessary);
2. lodge a report regarding the reportable situation to ASIC via the ASIC Regulatory Portal (the portal replaces previous methods for lodgement): https://regulatoryportal.asic.gov.au/

1. *When do we have knowledge?*

A person has "knowledge" of a circumstance or a result if they are aware that it exists or will exist in the ordinary course of events.[15]

2. *When are we reckless?*

A person is "reckless" if they are aware of a substantial risk that the circumstance exists or will exist, and having regard to the circumstances it is unjustifiable to take the risk.[16]

3. *What are reasonable grounds to believe?*

ASIC says that "reasonable grounds" to believe that a reportable situation has arisen exist where there are facts to induce, in a reasonable person, a belief that it's arisen. For example, if your compliance team knows that a breach has occurred but isn't sure that it's significant – it's still investigating – then that initial point in time of awareness of a breach is when the 30 days begins.

4. *Who has authority to make a decision about lodging reportable situation to ASIC?*

If a person has actual authority within their employment by Paul Melling & Associates Pty Limited to make a decision to lodge a breach report, the time at which that person has knowledge (or recklessness) is when the 30 days begins. The people within Paul Melling & Associates Pty Limited that have authority to make a decision to lodge a breach report are named at the beginning of this section. (However, see the note above about apparent authority.)

Ongoing analysis of breaches and reportable situations



An analysis of past entries in the Breach Register is important in ascertaining the spread, depth and trends of incidents, breaches, likely breaches and other reportable situations. From the analysis, systemic issues and inappropriate conduct can be identified, reported (if necessary) and corrected. The Compliance Manager will ensure analysis of past breaches occurs as necessary.

STEP 4: RECTIFY

Regardless of the whether the breach, likely breach or reportable situation is serious, we will rectify the matter and document how this is done in our Breach and Incidents register. Certain timeframes apply depending on the type of breach, likely breach or reportable situation.

Notifying clients affected by certain reportable situations

There are notification, investigation and remediation obligations that apply to us where:

1. personal advice is given to an affected client; and
2. a reportable situation (excluding 30+ day investigations) has occurred, including:
    - significant breach of a core obligation; or
    - gross negligence or serious fraud; and
3. there are reasonable grounds to suspect the client has suffered, or will suffer, loss or damage as a result of the reportable situation, and has a legally enforceable right to recover the loss or damage from the AFS licensee.

These obligations require us to:

1. Notify affected clients of the relevant misconduct within 30 days. ASIC says:

   The notice to affected clients must be in writing. It should explain the nature of the relevant reportable situation (the breach) and the basis for the suspicion that the affected client may have suffered or will suffer loss or damage. The types of information we consider are relevant to include in this notice are:
   • the date of the relevant reportable situation
   • a description of the relevant reportable situation
   • the consequences of the relevant reportable situation for the affected client and how they may be affected
   • relevant information about the investigation that is to be carried out
   • when the affected client should expect to hear from you next
   • their relevant consumer rights.

2. Investigate the nature and full extent of the misconduct. This includes updating clients along the way, and quantifying the loss or damage that affected clients have suffered or will suffer, or have a legally enforceable right to cover; and

3. Notify clients in writing of the outcome of the investigation, within 10 days of the completion of the investigation. ASIC says:

   This notice should:
   • explain the nature of the breach identified and any related breaches
   • describe how the breach affected the client's interests
   • assess the loss or damage you reasonably believe the affected client is entitled to seek to recover. Your investigation may find that an affected client you notified at [1 above] has not suffered or will not suffer loss or damage which they have a legally enforceable right to recover. If this is the case, you must still notify them of the outcome of the investigation as described above. In satisfying this obligation, a licensee has qualified privilege and is protected from a defamation action in relation to the information contained in the licensee's notice about the outcome of the investigation. The licensee is also not liable for any action based on breach of confidence.

4. If there is loss or damage and an enforceable right to recover, take reasonable steps to pay affected clients remediation of an amount equal to the loss or damage, within 30 days of the investigation concluding. ASIC says:

   For affected clients that you remediate, you may consider providing non-monetary remedies alongside the compensation provided. For example:
   • rescinding the contract
   • helping the client transfer to a more appropriate product
   • setting aside all or part of a debt owed by the client



Maintain records to show compliance with these obligations.

Notifying ASIC of other events

Notifying ASIC of other events

Representatives are trained in compliance obligations and are required to report any relevant event listed below to the Compliance Manager.

ASIC must be notified of any of the following events:

- any event that may make a material adverse change to the Licensee's financial position;
- change in control of the Licensee;
- change in the Licensee's name, principal business address or ABN;
- changing Responsible Managers, dispute resolution or compensation details;
- change in "key person" named on the licence;

- variation to authorisations and other conditions of an AFSL;
- authorising or revoking an authorised representative or financial adviser;
- changing a financial adviser or an authorised representative's name, principal business address, directors (if a company) or ABN;
- details of representatives providing financial product advice to retail clients;
- annual profit and loss statement and balance sheet;
- auditor report on the profit and loss statement and balance sheet;
- appointment of auditor (unless public company);
- consent to remove auditor;
- change of auditor;
- a licensee ceases to participate in a licensed market or a licensed CS facility; or
- notification of ineligibility to satisfy 'Broker Terms' criteria.



These events are set out in the Reporting Table Template: Lodgement Requirements for AFS Licensees (see below). The Compliance Manager is responsible for notifying ASIC of these events.

Some types of events and breaches must be reported to ASIC within a particular timeframe. Different periods of time and different fees and forms are associated with each event or breach. These requirements have been compiled into a "reporting table". These requirements change from time to time as the law and ASIC guidance change. Diarise to update the table once a year.

If an online form or portal limits the input of information in a way that risks the Licensee giving ASIC a misleading impression, the Licensee should clarify the information to ASIC separately in writing.

Reporting table



Please refer to the Reporting Table Template: Lodgement Requirements for AFS Licensees.

The Compliance Manager will:

- be familiar with which events must be reported to ASIC (listed above);
- contact the external compliance service providers for advice (if it is decided that this is necessary); and
- check the ASIC reporting table to determine when and how the information must be provided to ASIC.

Notification requirements under other regimes

Notification requirements under other regulatory regimes are outlined in the following internal documents:



Data Breach Response Plan

- Design and distribution – significant dealings

Related policies and tools

Policies	Client Review and Remediation, Risk Management.
Tools (including templates)	Breaches & Incidents Register, Compliance Diary & Checklist, Data Breach Response Plan, Reporting Table Template: Lodgement Requirements for AFS Licensees.

Keywords: breach reporting, reporting requirements.

Legislative requirements and references

Legislation	Sections 912D, s912DAA, 912DAB, 912EA, 912EB and 1317E of the *Corporations Act 2001* *ASIC Act 2001*
Regulatory guidance	ASIC's Regulatory Guide 78 Breach reporting by licensees[17] ASIC's Regulatory Guide 104 AFS licensing: Meeting the general obligations ASIC's Regulatory Guide 105 AFS Licensing: Organisational competence

Endnotes

[1] Section 912D of the Act
[2] Us as licensee (not our representatives) must have had reasonable grounds to believe that the other individual has engaged in conduct that forms part of the reportable situation.
[3] All the bulleted sections above and including this line refer to s912A of the Act.
[4] Section 912B of the Act.
[5] Special rules apply to Traditional Trustee Companies that we have not considered here.
[6] However, the civil penalty provisions in those Acts do not trigger a "deemed reportable situation" – see https://www.legislation.gov.au/Details/F2021L01072
[7] Section 912D(4)(a) of the Act (From 1 October 2021).
[8] See Section 1317E of the Act for a table that sets out civil penalty provisions.
[9] See explanatory memorandum: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6630_ems_4c5698fa-a114-4687-9843-595e795a64cf/upload_pdf/JC000444.pdf;fileType=application%2Fpdf paragraph 11.33
[10] See Explanatory Memorandum, paragraphs 11.30–11.33
[11] see Table 6 of ASIC's RG 78.57.
[12] See ASIC's Draft RG 78.64.
[13] Section 1100A or s912DAB(6) of the Act.
[14] Section 912DAB(7) of the Act.
[15] Section 5.3 of the Commonwealth Criminal Code.
[16] See Section 5.4 of the Commonwealth Criminal Code for more detail.
[17] https://download.asic.gov.au/media/1239857/rg78-published-26-february-2014.pdf.