stewart title®

Data Breach Response Plan January 2018

Maintain Information Governance and Security

Stewart has an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or Known Data Breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, that an entity holds.

Contain

Stewart's first step is to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Access

Stewart will consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If Stewart has reasonable grounds to believe this is the case, then Stewart must notify. If Stewart only has grounds to suspect that this is the case, then Stewart must conduct an assessment process. As part of the **assessment**, Stewart will consider whether **remedial action** is possible.

Stewart will follow a three-stage process for conducting an assessment:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. This decision will be documented.

Stewart will conduct this assessment expeditiously and, where possible, within 30 days. If it can't be done within 30 days, Stewart will document why this is the case.

Take Remedial Action

Where possible, Stewart will take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and Stewart will progress to the review stage.

NO — **Is serious harm still likely?** — **YES**

Notify

Where serious harm is likely, Stewart will prepare a statement for the Commissioner that contains:

- Stewart's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Stewart will also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1**: Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

Option 3: publish the statement on Stewart's website and publicise it

Stewart may provide further information in any notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Stewart will review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Stewart will also consider reporting the incident to other relevant bodies, such as:

- Police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- Professional Bodies

Stewart may also report the incident to other international authorities in accordance with any notification obligations Stewart may have under other breach notification schemes, such as EU General Data Protection Regulation.