**Date of Protocol:** 4/05/2020

**Version:** 1.1

# Data Breach Notification Protocol

## I. OVERVIEW

| | |
|---|---|
| **1. WHO MUST READ THIS PROTOCOL** | If you supply, access or otherwise deal with information or an opinion about an identified individual, or an individual who is reasonably identifiable:<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not, through or for Class **(Personal Information),** then this protocol applies to you and you are a **Data Entity.** |
| **2. WHY THIS PROTOCOL IS IMPORTANT** | Class software operates much like an "ecosystem". There are multiple participants in that ecosystem, including data providers such as fund managers, stock brokers and financial institutions, direct customers such as accountants and wealth advisers, and users that are invited in by others including trustees and beneficiaries, auditors and the like. As a result, a range of persons request, provide, access, use and disclose Personal Information using Class software, and that Personal Information may relate to, or have been provided by, themselves, their clients or other Data Entities.<br><br>We believe it is in the interests of all Data Entities that data breaches affecting Personal Information are identified, reported and managed. In part this is required so that Class and Data Entities can each comply with obligations they have to notify and manage data breaches. These may be obligations arising under the notifiable data breach scheme in the Privacy Act, or obligations assumed under contract.<br><br>Class has prepared this protocol to help ensure that it and all Data Entities:<br>(a) comply with the obligations they have in relation to data breaches under the Privacy Act and elsewhere ; and<br>(b) work together to minimise the impact of and protect against data |

## 3. ELIGIBLE DATA BREACHES

For the purpose of this protocol, an **Eligible Data Breach** occurs where:

(a) there has been either unauthorised access to / disclosure of Personal Information, or Personal Information has been lost in circumstances where there will likely be unauthorised access / disclosure (a **Data Breach**);

(b) a reasonable person would conclude these circumstances are likely to result in serious harm to an individual who has Personal Information relating to them at risk from the unauthorised access / disclosure **(Affected Individual)**; and

(c) remedial steps cannot be taken to either prevent the unauthorised access / disclosure before it happens or prevent the serious harm to the Affected Individuals before it occurs.

## 4. YOUR OBLIGATIONS

Each Data Entitv must:

(a) **notify:** immediately notify Class if it becomes aware of (or suspect that there has been) any unauthorised access to, disclosure or loss of, or any other unauthorised interference with, any Personal Information;

(b) **process:** comply with the process set out on page 2 of this protocol; and

(c) **confirmation:** provide Class with information reasonably requested to enable Class to test and validate its compliance with this protocol.

## 5. WHEN THIS PROTOCOL DOESN'T APPLY

A Data Entity does not have to follow this protocol where a Data Breach occurs which solely relates to Personal Information the Data Entity itself has provided.

Take, for example, an accounting firm who uses Class Super to manage a client's SMSF. If:

(a) the accounting firm fails to disable the access of one of their own employees who leaves their organisation;

(b) that employee improperly accesses that client's Personal Information in Class Super; and

(c) the Personal Information that is improperly accessed has been entered into Class Super by the accounting firm,

the accounting firm does not need to follow this protocol, and this will not constitute an Eligible Data Breach. This is because it is essentially an internal matter for the accounting firm.

If, however, the Personal Information has been provided by a third party, such as a data feed obtained from a funds manager or stock broker, this may constitute an Eligible Data Breach. This is because it may be appropriate for the funds manager or stock broker who provided the information to be informed of the Data Breach.

## 6. FURTHER RESOURCES

The Office of Australian Information Commissioner (OAIC): www.oaic.gov.au Privacy Act 1988 (Cth): https://www.legislation.gov.au/Details/C2017C00283

# II. Data breach notification process

## If you become aware of or suspect

Potential unauthorised access to or disclosure of Personal Information

OR

Potential loss of Personal Information in circumstances where unauthorised access to or disclosure of is likely to occur

OR

Any other unauthorised interference with Personal Information

## You must immediately

Notify Class of (i) the nature and details of the suspected Eligible Data Breach and (ii) any recommended initial steps to be taken in response

AND

Work with Class on the investigation and assessment of whether there are reasonable grounds to believe there has been an actual Eligible Data Breach

AND

Act to contain and mitigate the potential Eligible Data Breach, protect Affected individuals, and protect the Personal Information from further breaches

## If there is an eligible data breach

You must discuss and work with Class to investigate the Eligible Data Breach, including deciding on and implementing appropriate remedial and mitigating steps until remediation is complete and prevention plans have been implemented

AND

You must agree with Class who will manage the notification process, including deciding who will be responsible for notifying OAIC/relevant Affected Individuals if this is required

If you manage the notifications process, you must consult with Class, take into account Class' reasonable considerations, and obtain Class' approval prior to issuing the notifications

OR

If Class or another Data Entity manages the notifications, you must cooperate and provide reasonable assistance to Class or that Data Entity

If compliance here prevents your compliance with any applicable laws, you must at least provide Class with copies of the notifications/ statements as soon as practicable

You must generally cooperate with and provide all reasonable assistance to Class to ensure it complies with its legislative and contractual obligations in relation to an Eligible Data Breach

## After notifications and containing the breach

You must identify the cause of the Eligible Data Breach and take steps to prevent such an Eligible Data Breach from occurring again

You must provide Class with a written report detailing the cause of the Eligible Data Breach and your prevention plan

## III. EXAMPLES

| | |
|---|---|
| **1. POTENTIAL ELIGIBLE DATA BREACHES** | (a) A Data Entity fires an employee with access to Personal Information, but does not remove the employee's authorised access to, or change applicable passwords or other security around the Personal Information in a timely manner.<br>(b) A data file, laptop, smartphone, or other device containing Personal Information is sent to the wrong recipient or is otherwise lost.<br>(c) An application vulnerability on a Data Entity website, server or system allows access to Personal Information.<br>(d) Laptops, devices, software or applications used by Data Entities in systems that have access to Personal Information are critically out-of-date or are unencrypted.<br>(e) A Data Entity employee leaves hard copies of documents containing Personal Information in a customer or service provider meeting room, and that customer or service provider would not otherwise have access to that Personal Information. |
| **2. POTENTIAL REMEDIAL OR PROTECTIVE ACTIONS** | (a) Implement a policy ensuring that authorised accesses are revoked immediately when employees are terminated or otherwise leave. Reasonably refresh passwords and other security around the Personal Information from time to time.<br>(b) Immediately reach out to the recipient to notify them that they should not access the Personal Information and return or delete it, or ask the relevant IT support staff to remotely wipe the Personal Information form the device where possible.<br>(c) Run periodic checks for application vulnerabilities and security system reviews.<br>(d) Ensure devices and software are auto-updated, and relevant devices are encrypted.<br>(e) Immediately reach out to the customer or service provider that they must not read the documents and must store the documents in a safe place until the Data Entity employee can retrieve them. |