



CASE STUDIES – CYBER INCIDENT AND COMPLAINT HANDLING

RESPONSIBLE MANAGER TRAINING OCTOBER 2023

DISCLAIMER

This information has been prepared by Centrepont Alliance Limited.

This information is based on our understanding of current regulatory requirements and laws as at the presentation date. It is not intended to be a comprehensive statement and should not be relied on as such. You should form your own opinion and take your own legal, taxation and financial advice on the application of the information to your business if applicable.

Whilst all care has been taken in the preparation of this document (using sources believed to be reliable and accurate), to the maximum extent permitted by law, no person including Centrepont Alliance Limited or any member of the Centrepont Alliance Group of companies accepts responsibility for any loss suffered by any person arising from reliance on this information.

This presentation cannot be used or copied in whole or part without our express written consent.

LEARNING OUTCOMES

By participating in this session you will:



Understand how to prevent and respond to a cyber incident



Be able to assess and report a data breach

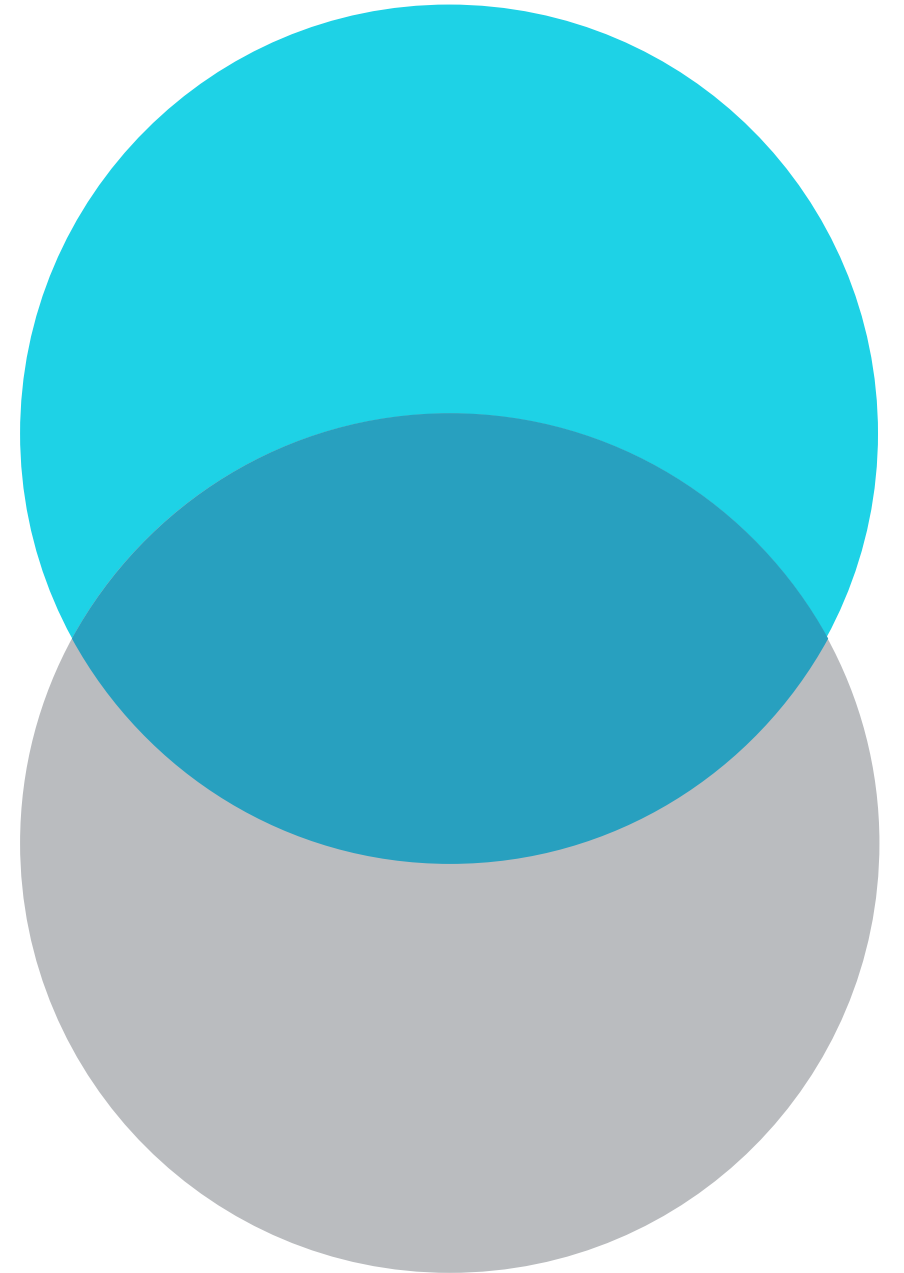


Implement an effective IDR process



Understand the IDR record keeping and reporting requirements

MANAGING A CYBER INCIDENT



ACSC ANNUAL CYBER THREAT REPORT

- Prevalence and cost of cybercrime
- Trends and threats



CYBERCRIME AS A SERVICE

Cybercrime as a service (CaaS) is evolving to encompass a range of purchasable tools, services and information. This includes the sale of access to compromised networks, malware developers etc so that a cybercriminal doesn't need to be a technical expert. As a result, cybercrime is becoming more specialised, harder to detect and pose a greater threat.

- There were 76,000 cybercrime reports in 2021-2022, an increase of 13%.
- The average cost of cybercrime for small businesses was \$39,000 per incident, an increase of 14%.

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is using email to target an organisation with the goal of stealing money or information. For example, using emails trick employees into paying fraudulent invoices, transferring funds or providing sensitive information.

May also include credential harvesting including where users are tricked into revealing their login details e.g. phishing, brute-force attacks or systems are compromised by malware

Once the malicious actor has access to the person's email they can:

- Access emails sent or received, and the information contained in emails or attachments
- Access contacts and send malicious emails from your account
- Set rules in the email account such as BCC themselves on future emails, or delay and alter emails being sent
- Sell the credentials

- BEC trended towards targeting high value transactions.
- Losses for BEC was an average of \$64,000 per incident.
- Only a small fraction of BEC losses are ever recovered.

SYSTEM VULNERABILITIES

System vulnerabilities are a key target for cybercrime. Once a security vulnerability is known it is expected that malicious code will be developed within 48 hours. Businesses should prioritise automated updates and ensure patching is done within 48 hours. Malicious actors are scanning networks for unpatched systems, seeking to use these as entry points. Most incidents were due to inadequate patching.

- 25% increase in publicly reported software vulnerabilities.
- ACSC estimates 150,000 to 200,000 Australian homes and businesses are vulnerable.

CASE STUDY

- Phishing and Social Engineering
- Business Email Compromise and Credential Harvesting



HOW THE INCIDENT WAS DISCOVERED



CSO sends an email to the client to confirm that his withdrawal request has been processed.




CSO receives a call from the client to say he didn't request a withdrawal.



CSO has been corresponding with this client about his withdrawal and is confused.

THE LEAD-UP



- CSO received a client email forwarded by the adviser asking to arrange a \$200,000 withdrawal from the client's super fund.



- The CSO arranged the withdrawal, replying to the email trail.



- The client requested a change of bank account for the payment, which the CSO arranged.



- CSO received a second request directly from the client asking for another \$250,000.



- CSO emailed the client to confirm the withdrawal using the client's email address obtained from their CRM.

HOW DID IT HAPPEN?

- Months prior, the adviser received an email from a digital signature provider that he used frequently.
- The adviser clicked on the link, was redirected to an Office365 login. The adviser entered their account information.
- The adviser also entered their MFA code when prompted.
- Nothing happened and the adviser forgot about it.
- The bad actor now had access to the adviser's email including the cookie for their MFA.
- The bad actor located a withdrawal form for \$20,000 on an old email.
- The bad actor created a fake email account and sent an email to the adviser, and then forwarded that email to the CSO before deleting both emails.
- From this point the bad actor dealt with the CSO directly using the information gained in the adviser's email.

ACTIVITY

Discuss:

- What went wrong?
- How could it have been prevented – procedures and technical measures?



PREVENTION

- Procedures for actioning and verifying client requests
- Technical measures



PROCEDURAL AND TECHNICAL VULNERABILITIES

- The CSO assumed the adviser had verified the withdrawal with the client
- The CSO didn't check the email address
- There was no discussion between the CSO and the adviser
- There were no phone calls between the CSO or adviser and the client
- Client information being sent via emails
- Not using secure portals
- The adviser was vulnerable to a phishing attack
- Lack of email and content filtering?

PROCEDURE CHANGES

- Implement a call back policy. Always call a client to confirm email instructions.
- Don't change bank accounts or update contact details on instructions via email, always call
- Check and use the phone number and email address from your CRM not those provided in the email
- Keep a file note of confirmation phone calls
- Support staff should not act on an email from an adviser without verbal instructions or checking the confirmation file note
- 2-person approval process for withdrawals above \$X – verify the email address, signatures, bank account details

PREVENTATIVE MEASURES

- Password protecting documents - Password protection was implemented 6 months earlier, but the bad actor had access to years' worth of emails.
- Email policy - Emails were not deleted or archived. Emails should be uploaded to CRM and deleted from email. Email should be archived after a set period.
- Using secure portals – better than password protection
- Email filtering - SMTP gateway was used but the sender was not flagged as suspicious by the provider.
- Content filtering - The practice had content filtering, but this site has not had any prior reports that would flag it.
- MFA - was in place but cookie was captured from the Office365 login during the phishing attack
- Education - Don't click on links. Beware of session hijacking. Navigate directly to known websites.

INCIDENT RESPONSE

- Documentation and preparation
- Actions taken to respond to the incident



ACTIVITY

Discuss:

- How would you respond to the incident?
 - What steps would you take immediately?
 - What resources can you access?
 - What investigation would you do?



IS A CYBERSECURITY INCIDENT AND A DATA BREACH THE SAME?

“Cyber security incidents continue to have a significant impact on the community and were the cause of the majority of large-scale breaches.”

Australian Information Commissioner and Privacy Commissioner Angelene Falk

Cybersecurity Incident

A cybersecurity event is, an event affecting systems, service or network security, that has (or may) compromise business operations.

It may be caused by a malicious attack, a failure of safeguards, or violation of policies.

Data Breach

A data breach is the unauthorised access or disclosure of personal information, or loss of personal information

It may be caused by malicious action, human error, or a failure in information handling or security systems.

CYBER INCIDENT RESPONSE PLAN

- Internal roles, responsibilities and contact details
- Stakeholders, external expertise and contact details
- Procedures and playbooks
- Incident response process
 - Detect, investigate, analyse
 - Contain, collect and preserve evidence, remediate
 - Recover
 - Post incident review, changes and training
- Incident notification and reporting obligations
 - Regulatory requirements
 - Insurance policy details



CYBER INCIDENT RESPONSE PLAN

TEMPLATE

cyber.gov.au

INCIDENT RESPONSE PROCESS

Investigate

- What expertise and resources are required?
- What systems have been compromised?
- What post-exploitation activity has occurred?
- Do they still have access?
- Has data been accessed or exfiltrated?


Contain

- Can access to, or distribution of, information be limited?
- Collect and preserve all evidence

Remediate

- Actions required
- Responsibilities and timeframes

Document the incident and the response



**You will need
technical expertise. It
is important not to
destroy evidence
needed to investigate.**


CYBER INSURANCE

Cyber insurance policies may cover:

- Third party claims for failure to keep data secure
- Third party losses from funds transfer fraud and social engineering
- Reimbursement of your costs to respond to and recover from a cyber incident or data breach
- Cyber extortion costs
- Business interruption compensation

Additional benefits may include:

- Incident response handling by experts
- Free security upgrades



If you have a cyber policy, contact the provider immediately so that you do not invalidate the policy.

DATA BREACH RESPONSE PLAN



What a data breach is



Roles and responsibilities



External expertise



Strategies for containing and remediating data breaches



How to assess a data breach



Notification procedures for individuals and OAIC



How to document incidents



Requirements of other parties such as service providers or insurers



Post breach review of the response

DATA BREACH RESPONSE

Notify the Privacy Officer

- A description of the breach
- When the breach was discovered
- When the breach occurred
- The type of personal information involved
- The cause of the breach
- The individuals affected
- Any immediate steps taken to contain or remediate the breach

Response by the Privacy Officer and Data Breach Response Team

- Consider the type of potential harm – identify theft, financial loss etc
- Consider whether the actions taken likely prevented the risk of serious harm
- Consider further actions required – as part of the investigation or remediation
- Determine if it is a notifiable data breach
- Review and take action to prevent future breaches
- Keep records

REPORTING

- Obligation to report
- What to include in reports and notifications



ACTIVITY

Discuss:

- Would you report this incident?
 - To whom?
 - What information do you need to assess the incident?
- Would you notify clients?
 - Which clients?
 - What would you include in any communication?



INVESTIGATION

The hacker had access for 6 days and reviewed emails containing the personal information of 25 individuals.

Each email was reviewed to determine the information it contained. Information included:

- Names, DOB, addresses, contact details
- Account numbers – product, bank accounts, loans
- Account balances
- Signatures
- TFN, tax statements, payslips
- Medical information
- Forms – withdrawals, applications
- Fact find, SoA
- Emails from referral partners with prospective client details



NOTIFIABLE DATA BREACHES

The NDB Scheme applies to entities that have obligations under the Privacy Act such as AFS Licensees.

You must notify affected individuals and the OAIC when a data breach is **likely to result in serious harm**.

Whether a data breach is likely to result in serious harm requires an objective assessment. ‘Serious harm’ is not defined but may include serious physical, psychological, emotional, financial, or reputational harm.

The types of information that is more likely to cause serious harm includes:

- Sensitive information such as health information
- Documents/information that can be used for identity theft such as driver’s licence, Medicare cards or passports
- Financial information including account details, TFN, transactions
- Information that when combined with other information can cause harm such as names and contact details.

If remedial action prevents serious harm, notification is not required.

Report online - <https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach>

NOTIFIABLE DATA BREACH FORM

Information that is included in the report is:

- Description of the breach
- Information involved in the breach
- What steps the individuals affected should take to reduce the risk of harm
- Date occurred & discovered;
- Cause of the breach e.g. malicious or criminal attack/social engineering
- Number of individuals affected
- How the breach occurred
- Remedial action
- Action to prevent a future breach
- How and when individuals will be notified
- Other bodies this was reported to
- Copies of notifications to individuals

CLIENT NOTIFICATION

Information to include in a client notification

- What happened
- Information affected
- What the individual should do to protect themselves – e.g. change passwords, review transactions, inform financial institutions
- What the adviser and licensee has done
- Who to contact in the event of a complaint – adviser, licensee and OAIC

ACSC CYBER REPORT

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) leads the Australian Government's efforts to improve cyber security.

You can report a cybercrime, cyber incident, or cyber vulnerability at www.cyber.gov.au/report. Reporting assists the ACSC to combat cyber threats to Australia. The report is passed onto law enforcement for assessment and intelligence.

Information that is included when reporting an incident:

- The original phishing email purporting to be from the digital signature provider was reported to ACSC. Details of the email address including the email, IP address, and website link.
- Provide details of the subsequent activity including the fraudulent email (pretending to be the client) and the electronic funds transfer that resulted.
- The outcome, the amount of money recovered.

CASE STUDY

- Action taken
- Outcome



HOW THE BREACH WAS RESOLVED

- The product provider was contacted and was able to stop the second payment immediately. Only a portion of the first withdrawal was able to be recovered.
- The adviser contacted their cyber insurance provider who appointed an expert to ensure the breach was contained and to conduct a forensic investigation.
- Affected clients were contacted by phone and received an email explaining the action they should take to protect their information.
- Reports were submitted to the ACSC and the OAIC. The OAIC as satisfied with actions taken.
- The client was compensated by the product provider. Responsibility for reimbursement is being determined.

LICENSEE OBLIGATIONS

- Privacy
- Adequate technology resources



OBLIGATIONS AND CYBERSECURITY FRAMEWORK

Privacy

Licensee's and their representatives receive and store electronically, confidential and sensitive client information and must have adequate systems, policies and procedures in place to protect this information from misuse, interference and loss, from unauthorised access, modification or disclosure.

Adequate technology resources

Your cybersecurity framework must incorporate a range of measures to prevent access to your network by exploiting vulnerabilities in your systems or people; and enable you to respond to and recover from cybersecurity events.

Cybersecurity measures may include:

- Policies to address secure storage and sharing of information
- Tech measures such as a firewall, patching systems, access & password management, MFA, data back up, web and email content filtering
- Education and training
- External assessment of IT systems

NEXT STEPS



Review your cyber security measures and policies. These will help to protect against a cyber-attack.



Review your procedures and provide staff training. People are key to protect clients and your business.



Document your Incident Response Plan and Data Breach Response Plan. These will ensure you are prepared to respond to an incident.



Consider Cyber Insurance. It will help you to respond to and recover from an incident, as well as cover costs and losses.

PSC INSURANCE BROKERS

David Withers

Managing Principal

M: 0423 489 847

E: dwithers@pscinsurance.com.au



Brooke Gunasti

Account Executive

M: 0448 765 286

E: bgunasti@pscinsurance.com.au



PSC INSURANCE – CYBER POLICY PRICING

Total Cost including charges based on VIC, WA, NT

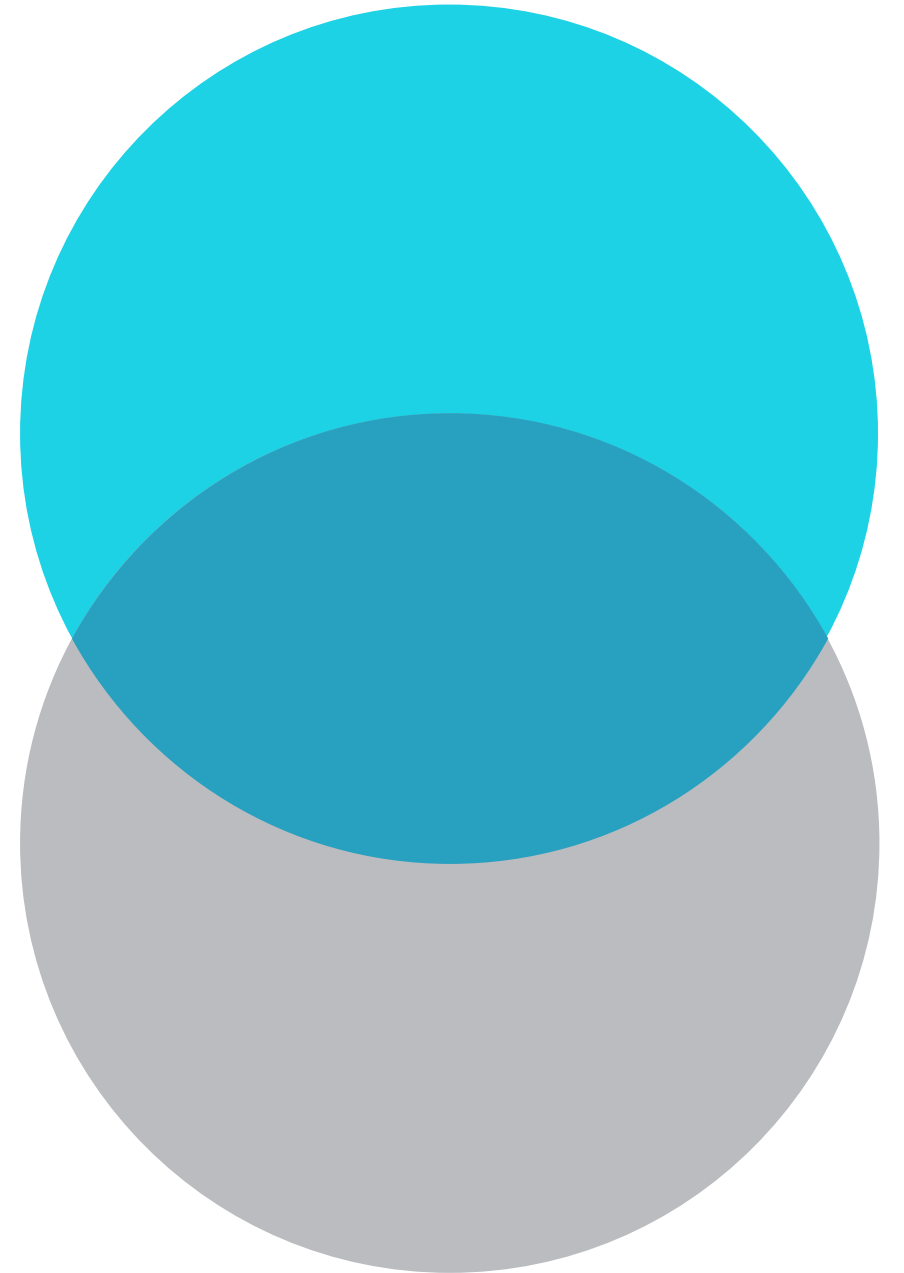
Option A - \$1,000 Excess

	\$	250,000.00	\$	500,000.00	\$	1,000,000.00
<\$100k		\$777.48		\$1,078.13		X
\$100k-\$250k		\$947.47		\$1,170.73		X
\$250k-\$500k		\$1,015.97		\$1,234.16		\$1,617.26
\$500k-\$1M		\$1,092.08		\$1,326.76		\$1,801.20
\$1M-\$1.5M		\$1,191.03		\$1,563.98		\$2,068.87
\$1.5M-\$3M		\$1,316.62		\$1,783.44		\$2,250.27
\$3M-\$5M		\$1,671.80		\$2,313.70		\$2,955.58

Option B - \$2,500 Excess

	\$	250,000.00	\$	500,000.00	\$	1,000,000.00
<\$100k		\$745.48		\$1,031.10		X
\$100k-\$250k		\$906.98		\$1,119.06		X
\$250k-\$500k		\$972.05		\$1,179.32		\$1,543.27
\$500k-\$1M		\$1,044.35		\$1,267.30		\$1,718.01
\$1M-\$1.5M		\$1,138.36		\$1,492.65		\$1,972.30
\$1.5M-\$3M		\$1,257.67		\$1,701.15		\$2,144.64
\$3M-\$5M		\$1,595.09		\$2,204.88		\$2,814.67

MANAGING A COMPLAINT



DEFINITION

A complaint is defined as an “**expression of dissatisfaction** made to, or about, an organisation, related to its **products, services, staff or the handling of a complaint**, where a **response or resolution is explicitly or implicitly expected** or legally required.”

Common disputes may be about the following:

- Service – quality of service, treatment by staff
- Actions or decisions – incorrect or unfair, not properly explained. Includes inappropriate or insufficient advice.
- Inaction or delay – not responding, delay in providing service, not explaining a delay
- Policy and processes – disagreement, lack of explanation. Includes misleading or insufficient information.

A complaint is not:

- An opinion unless a resolution is expected or should reasonably be provided
- Requests for information, explanation or an update*
- A request for action to be taken*

* *Repeated requests may be a complaint*

CASE STUDY

- Fee and service complaint (with a twist)



THE COMPLAINT

I am writing to you to seek your review of fees paid for services not rendered that have impacted my investments for the past 18 months.

On several occasions I had emailed and voiced my concerns at the lack of service or advice during the period April 2020 to March 2023.

Also, I find myself in a challenging position having to declare to false statements that were made on the application for my income protection insurance prepared by (adviser) due to oversight and negligence.

I formally request a review of the fees charged for the period April 2020 to March 2023.

Ms K

ACTIVITY

Discuss:

- What actions would you take immediately?
- How would you reply to the complainant?
 - Are there any key points you should include?



IDR PROCESS

- Acknowledge within 1 day
- Investigate
- Resolve within 30 days



DAY 1

- Start a file and keep copies of the correspondence
- Make a file note of the conversation (if a phone call)
- Check that the licensee is responsible for the complaint - check the relevant dates
- Download the file immediately
- Notify relevant parties – internal and PI insurer
- Notify the relevant CAR/Adviser
- Acknowledge the complaint - you do not need to provide a resolution or deny the claim.
- Ask for more information from the complainant (if required)
- Add to the Complaint Register
- Add due dates to your diary/calendar



**Don't 'fire off' an
emotional reply**

**Do refer to the
Dispute Resolution
Procedure**

TEMPLATE ACKNOWLEDGEMENT LETTER

Complaint against [Licensee] and [Adviser Name] Ref: [insert reference number]

Dear [Name of claimant],

Thank you for contacting [us/AFCA] on [insert date on email/letter/phone call] to raise a complaint against our authorised representative [insert adviser's name].

As the holder of an Australian Financial Services Licence, we have obligation under the Corporations Act, including to deal with complaints fairly and efficiently. We take those obligation seriously and we have an internal dispute resolution process for the handling of complaints. We will endeavour to resolve your complaint directly with you.

[If applicable] We request that you provide the following information to assist us to investigate and resolve your concerns:

[insert information requested]

We will conduct a thorough investigation into your complaint, which will generally include interviewing your adviser and obtaining a copy of your file from your adviser. We will keep you informed of the progress of our investigation and contact you if we require additional information.

Following the completion of our investigation a full response will be provided to you. It is anticipated this will be no longer than 30 days.

ACTIVITY


Discuss:

- What investigation would you do?
 - What standard actions should be undertaken?
 - What is unique for this complaint?



INVESTIGATION

- Seek information from the complainant including the resolution sought (if not known)
- Prepare a timeline in chronological order all interactions and documentation on the file
- Review the file including advice documents, OFA
- For the relevant period obtain a revenue report
- For the relevant period obtain a transaction list
- Interview the adviser / seek a response addressing the allegations.
- Seek legal advice if required
- Keep the complainant informed of progress



**Obtain information
about the 'false
statements' on the
insurance application**

WHAT WAS FOUND

Fees and Services

- Found that the adviser had provided the services as per the OFA and no breach of service obligations.
- The adviser had given the client a partial refund of fees for one year.

Insurance

- The client had group insurance with her employer and took up a continuation option in 2020.
- Continuation cover was only available if the applicant was working for 15 hour+ per week. The client was unemployed from April 2020 to September 2020 and was therefore not eligible for the continuation option.

What is your current (new) occupation?

~~Not working yet~~ Admin

- On receiving the application form, the insurer queried the amendment with the client who confirmed that they were employed.
- There was an email from a CSO to the client that said “after discussing with (adviser), she will put you down as working”

ACTIVITY

Discuss:

- What actions would you take now?
- What is a suitable remedy/response?
- What would you say in your IDR response letter?



RESPONSE

Response may be either:

- Offer of a remedy; or
- Rejection of the complaint

Time limits

If unable to resolve within 30 calendar days, and IDR Delay Notification can be provided with the reason for delay and rights to complain to AFCA.

IDR Response Letter

- State each issue raised in the complaint
- Explain the circumstances and factors that were considered
- Explain your findings and information that supports the findings
- State your decision / remedy / actions taken and reasons (including reasons for rejection if applicable)
- If compensation is offered explain how it was calculated
- The right to complaint to AFCA if not satisfied and AFCA contact details

REMEDIES

- An explanation of the circumstances giving rise to the complaint
- Monetary compensation
- Goodwill payment
- A letter of apology
- Provision of assistance and support
- Refund or waiver of a fee or charge
- Replacement or rework e.g. new advice/review at no cost
- Correcting incorrect records
- Changing the terms of a contract
- Improvements to systems or procedures (or an undertaking to do so).

COMPENSATION

The purpose of compensation is to **place the client in the financial position in which they would have otherwise been** except for the:

- Inappropriate advice such as investments not suitable for the client's risk tolerance
- Failure such as implementation errors or delays, or failure to cancel insurance policies.

Calculating financial loss

1. Actual financial loss (where possible); or
 2. Assumptions; or
 3. Prescribed rates (if the above is not suitable)
- Insurance Contracts Regulations requires 10-year Australian Government bond rate plus 3%.
 - Reserve Bank of Australia (RBA) cash rate plus 6% recommended by ASIC

TEMPLATE IDR RESPONSE LETTER

Complaint against [Licensee] and [Adviser Name] Ref: [insert reference number]

Dear [Name of claimant],

We refer to your complaint against our authorised representative [insert adviser's name] on [insert date on email/letter/phone call].

Your Complaint

Based on your [email/letter/phone call], you have raised the following issues:

(List the issues raised by the claimant)

Our Investigation

To ensure that your allegations were addressed thoroughly, we reviewed your client file and the actions taken by the Adviser to allow us to identify what events transpired and if Adviser conduct has caused any financial loss or detriment to you.

Overview

(Describe the facts of the matter - set out what happened and when)

Our Findings

(Respond to each of the listed issues raised by the claimant)

TEMPLATE IDR RESPONSE LETTER

Our Resolution

Without any admission of legal liability, [Licensee] is willing to offer you total compensation of [settlement] to resolve your complaint in full and final settlement. The basis of calculation of this compensation amount is [insert basis and summary of the calculations].

Conclusion

Please note that this offer and any subsequent settlement is made on condition that you maintain it in the strictest confidence.

If you wish to accept this offer, please respond in writing by email to me by [date]. If you need more time to consider this offer please let me know. If you accept our offer we will require our standard Deed of Settlement to be executed with payment then being made to your nominated bank account within 30 days of receipt of the signed Deed of Settlement.

This is our final offer.

Your Rights

Our internal dispute resolution process has finished. If you are not satisfied with our final response, you may lodge a complaint with the Australian Financial Complaints Authority ('AFCA').

HOW THE COMPLAINT WAS RESOLVED

- The insurer was contacted during the investigation, and they made further enquiries about the circumstances of the original misrepresentation and the client's current employment.
- After a review the insurer decided not to take further action and confirmed in writing that they would honour the income protection policy.
- The licensee rejected the claim.

RECORD KEEPING, REPORTING

- Complaint register
- IDR Reporting to ASIC
- Assessing for breaches



RECORDING INFORMATION ABOUT COMPLAINTS

Firms are required to record all complaints and be able to track progress.

Complaint Register

- Complainant
- Adviser/CAR
- Summary of the complaint
- Date Acknowledged
- Date of IDR Delay Notification
- Date of IDR Response Letter
- Summary of actions taken, dates, updates, outcome
- Assessed for breaches
- Notified to PI insurer

IDR DATA REPORTING

- Licensees must report on complaint data every 6 months.
- Report complaint data for 1 July - 31 December 2023 by 29 February 2024
- Report even if there were no complaints.
- Report via the ASIC Regulatory Portal
- The information must be provided in a specific format and using specific codes.
 - Information about the complainant – gender, age, postcode
 - Date received and closed
 - The product/service
 - Complaint issue
 - Outcome
 - Compensation amount

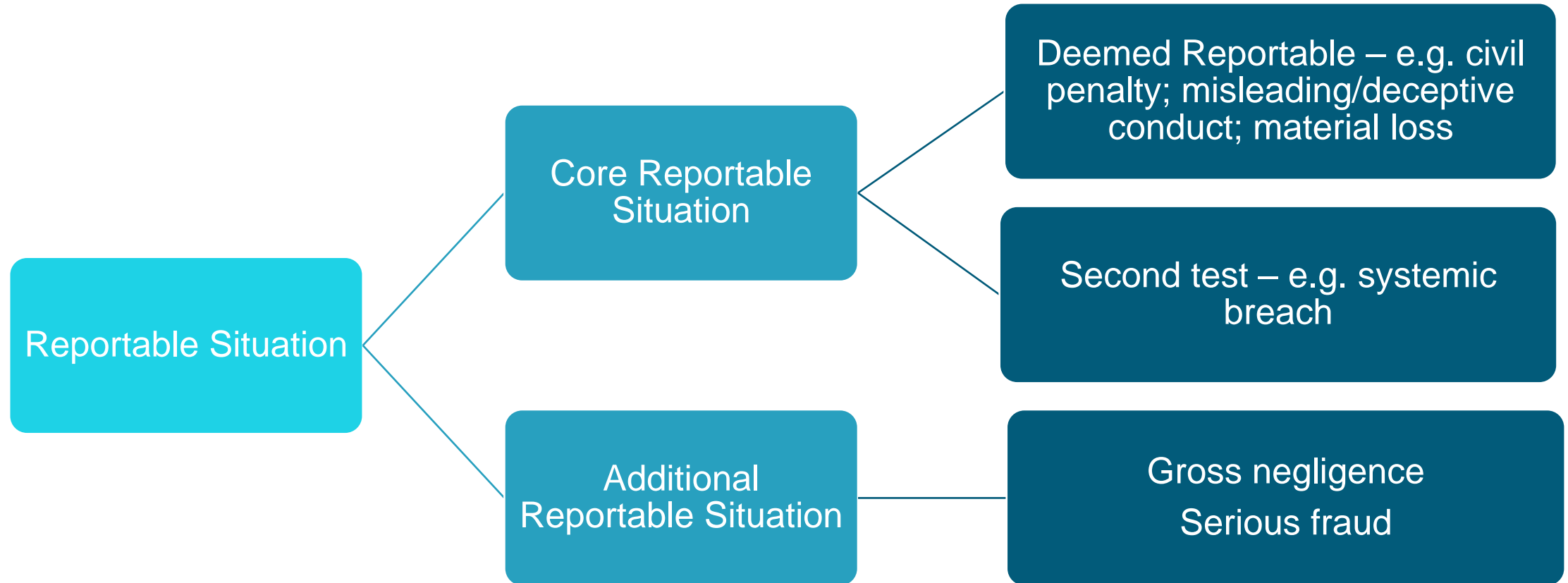
ACTIVITY

Discuss:

- Are there any breaches?
- If yes, is the breach a reportable situation?



BREACH ASSESSMENT



- Reported as serious fraud / misconduct

NEXT STEPS



Review your IDR Procedures and ensure staff are trained.



Ensure your complaint register is up to date and data is recorded as per ASIC IDR Reporting requirements.

THANK YOU

Questions

