

# Criminal conduct inside your organisation

Legal information for community organisations

---

## This fact sheet covers:

- ▶ what to do if you suspect that criminal conduct has occurred in your organisation, and
- ▶ examples of cases involving not-for-profit or charitable organisations

---

## This fact sheet aims to provide Australian not-for-profit community organisations with:

- a list of things to consider if you suspect criminal conduct is occurring within your organisation, and
- case studies which demonstrate not-for-profits are not immune from criminal conduct and that appropriate safeguards need to be put in place to protect against criminal conduct



### Note

This fact sheet provides general information about criminal conduct. This information is intended as a guide only and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before making a decision about what to do.

Please refer to [the full disclaimer](#) that applies to this fact sheet.



### Caution

Criminal conduct is very serious. If your organisation is experiencing an emergency (for example, you believe someone to be in direct harm), call 000.

If no one is in imminent danger or harm, we recommend organisations take the steps outlined in this fact sheet.



## What should you do?

If you suspect that there is criminal conduct taking place in your organisation, or you have been alerted to allegations of criminal conduct, **consider taking the following steps**:



### Note

The order in which you carry out these steps may vary depending on the individual circumstances (discussed in more detail below).

## Check your facts and investigate

First, try to make sure your suspicions, or the allegations you have been alerted to, are correct.

Given the seriousness of the suspicions, or allegations that form the subject of the enquiries, it's often difficult to determine what type of investigation is required.

### Consider policies in place

If the organisation has a policy (or procedure) which sets out how to handle criminal conduct (for example, a violence and harassment policy or a whistle-blower policy) it's important that you review the policy and follow the appropriate steps for reporting and investigating a complaint made under the policy.

For example, if an employee reports criminal conduct, your organisation may need to protect the identity of a reporter and prevent any harm to the reporter from the organisation or other employees under a whistle-blower policy.

Such policies are put in place in order to ensure fair treatment and protection to all parties involved. Accordingly, it is often a useful tool to start with.

If there is a policy in place but it's not followed, there may be arguments at a later date by either the accuser or the victim regarding impartiality of the investigation, privacy concerns or procedural fairness (or any combination of these things).

### The investigation

Typically, the investigation should be proportionate to the alleged conduct. There is not a 'one size fits all' process in terms of the investigation necessary following alleged criminal misconduct.

For example, in some instances it may be appropriate for an impartial party inside the organisation to carry out an investigation. However, in other instances, it may be necessary to enlist a neutral external party to carry out an investigation.

Factors to consider in determining whether an internal or external investigation include:

- If there are suspicions someone is being harassed or threatened, has that person confirmed that's what happened and that they want to take it further?



- What does the policy provide for (if one exists)?
- Is there an internal person who is impartial and objective with the required training to carry out the investigation?
- How serious and complex are the allegations?
- What level is the employee who is being investigated (ie. a subordinate should not investigate their superior – an external investigator would be more appropriate in that case)?



## Tips

- Ensure you have appropriate reporting channels in place. For example, who would someone tell if they saw something illegal or suspicious?
- Avoid putting anyone at risk by going straight to the police if you think there is a risk of harm to anyone.
- Document concerns by making sure file notes are kept of conversations or incidents. Ask relevant people to write down in their own words what has happened and what they think that means.
- Investigate if records support suspicions. For example, do the financial statements indicate that there are funds missing without authorisation or reimbursement claims for inappropriate reasons?
- If there are suspicions someone is being harassed or threatened, has that person confirmed that's what happened and that they want to take it further?

## Call the police

If the situation is an emergency, call 000.

Otherwise, call the Police Assistance number (for all states and territories with the exception of Victoria) on 131 444. In Victoria, from Monday to Friday, 8am to 4pm on: (03) 9247 6666.

## Call your insurer

Your organisation may have fidelity or fraud insurance, or a directors' and officers' insurance policy which covers your organisation in this situation. If this is the case, read the policy carefully and notify your insurer immediately if you think it applies.

If you try to make a claim later and didn't notify the insurer when the incident occurred, you may not be covered.

Coverage under each insurance policy will depend on the particular terms and conditions of each policy. It's important to contact your insurer as soon as you can after learning of facts or circumstances which may give rise to a claim.

Often, insurance companies have a panel of lawyers to assist with specific legal issues and you may be referred to one of these for further help.



## More information

For more information about insurance, see our [guide to insurance and risk management](#).



## Caution

It's important that you don't admit to anyone outside of your organisation that you are liable (responsible) for a potential claim without first speaking with both a legal representative (as discussed below) and your insurer. If you make an admission which is not approved in advance by your insurer, you may find you are stripped of insurance cover.

## Seek legal advice

Make sure your organisation approaches serious situations in the right way. Enlisting the assistance of lawyers early may help reduce the risk of complaints regarding breach of privacy and procedural fairness during investigations.

## Make sure the right people know - but be careful who you tell

The board or committee of management should be informed about suspected criminal conduct, depending on the expert advice you receive. Check this with your lawyer.



## Caution

There may be reasons that you should not inform all staff or volunteers of suspected criminal conduct, for example:

- you may put staff at risk
- you could open yourself to a defamation claim, or
- you might be in breach of your legal obligations with respect to privacy



## Case example – finance manager guilty of fraud

Ms Mooney was employed as the finance manager at not-for-profit organisation Transport Industries Skills Centre Inc (**Centre**).

While the Centre's payroll processing software required two signatures from authorised persons, Mooney had access to the CEO's security USB, as well as his e-signature (for emailing purposes). She used these and a company credit card to fraudulently authorise overpayments to herself and finance an unauthorised loan agreement for a motor vehicle.

While all personnel were required to submit receipts that established proper use of the credit card for all payments, the Centre's software pooled all credit card expenditure into a single account, making it hard to establish the legitimacy of individual transactions.

Nonetheless, Mooney was convicted of offences relating to the misappropriation of funds (which exceeded a total of \$157,000 over four years) and sentenced to three years imprisonment.

*R v Mooney [2017] ACTSC 358*



### Case example – audit reveals history of fraud

In this case, the offender was the chief financial officer of the Canberra Police Community Youth Club (**CPCYC**), a not-for-profit organisation that facilitated interaction between police officers and young people. As CFO, the offender managed all accounts held by the CPCYC, most of which she was authorised to do on her own and without the need for a second signature.

In 2015 (some four years after the offender's employment at CPCYC) an investigation of the accounts of CPCYC highlighted the existence of overdue reminders, letters of demand and some suspended and cancelled accounts. A more detailed investigation and a subsequent police investigation revealed the nature and extent of the offender's illegal transactions, which included (among other things) the transfer of funds from the CPCYC into her own account, the deposit of cheques into her own account, and withdrawal of money from ATM's using the CPCYC account. Each of these appropriations were done without the permission of her employer, and amounted to a total of \$406,875.

The Court was of the view that these transactions were made in pursuit of satisfying the offender's gambling addiction.

Although the systems of CPCYC in relation to monitoring the company's financial position were not really considered in this case, it's clear there are some similarities between this case and that of Mooney (above). In particular, the offender was largely given free-reign when it came to the authorisation of most transactions, without the requirement for approval of a second person of authority.

The Court imposed a sentence of three years, which was to be suspended after a period of 15 months.

*R v NQ [2017] ACTSC 317*



### Case example – funder uncovers fraud

Mr Matcham was the CEO of Katungul Aboriginal Corporation Community and Medical Services (**Katungul**), a not-for-profit Aboriginal owned and controlled entity.

Over a period of time, a Katungul board member questioned Mr Matcham at board meetings about his concerns regarding Katungul's position, its finances and other issues concerning the quality of the services it was providing.

A funder of Katungul, the Commonwealth Office of Aboriginal and Torres Strait Islander Health conducted an audit of Katungul's financial records on the basis of these concerns.

Following the audit, it was discovered that Mr Matcham had made a large amount of unauthorised payments to himself (totalling more than \$700,000).

The finance manager hadn't check the accuracy of hours Mr Matcham recorded in his timesheets (which, at one point, indicated that he was working over 24 hours per day).

The Court found Mr Matcham abused his position of trust by obtaining large payments to which he was not entitled, and which were acquired for his personal use. Given the payments were authorised by him over a period of four years, the Court was also satisfied that he was aware of the fact that he was not entitled to the payments without board approval. The unauthorised payments obtained by Mr Matcham contributed to Katungul's parlous financial position, depriving the Indigenous community of health care services.

The Court ordered that Mr Matcham:

- pay back Katungul in the amount of \$705,905.07
- be disqualified from managing Aboriginal and Torres Strait Islander corporations for a period of 15 years, and
- pay the Commonwealth a penalty of \$500,000

*Registrar of Aboriginal and Torres Strait Islander Corporations v Matcham (No 2) [2014] FCA 27*



### Case example – principal officer of two NGOs involved in fraud

Ms Sharobeem, was the principal officer of the Immigrant Women's Health Service (IWHS) and the person in day-to-day charge of Non-English Speaking Housing Women's Scheme Inc (NESH), both not-for-profit entities.

IWHS' auditor reported concerns about Sharobeem's conduct to the South Western Sydney Local Health District (SWSLHD), a public authority that funded IWHS. SWSLHD report this to ICAC, which investigated.

ICAC's investigation found that Sharobeem improperly exercised her official function at IWHS and NESH to misuse up to \$773,000 of public funds to benefit herself and members of her family. It was alleged Sharobeem claimed and authorised reimbursement from IWHS and NESH for non-work related expenses such as refurbishment work on her property and liposuction for her son. It was also found that she used IWHS and NESH credit cards for personal expenses such as purchasing a Mercedes car and a massage chair.

Due to the limited funding received by both organisations, the misuse of funds represented a substantial amount of public funds given to those organisations for public purposes.

ICAC found that Sharobeem engaged in 24 serious corrupt conduct findings and recommended the Director of Public Prosecutions advise on her prosecution.

*Investigation into the conduct of a principal officer of two non-government organisations and others (2018)*. NSW Independent Commission Against Corruption.