FRAUD WITHIN THE SUPPLY CHAIN INDUSTRY
DETECTION AND RECOVERY

FCB

MATTHEW ROBINSON, Partner, and CERI WILLIAMS, Solicitor, both of FCB Workplace Law, examine the trends and implications of employee theft in the manufacturing and logistics industries to identify best-practice approaches to detecting, combatting and resolving supply chain fraud.

Fraud is the by-product of human greed. There is little any business can do (other than hiring robots) to stop criminals from committing some level of fraud or theft from your workplace. You would think that good hiring practices should root out the obvious characters, however most of the sizeable frauds are perpetrated by people least suspected: Executives & Senior Managers. These managers look unremarkable, they blend into the business, they are sociable, helpful but like to remain the point of control of their function or business line.

Most people are content to work within their company's prescribed systems though some can be tempted to commit fraud where they spot an opportunity within weak systems and controls and/or there is some convertible value for the products coming in and out of their link in the supply chain. Weak systems and low levels of managerial oversight occur in all industries, however the Supply Chain industry has a heightened fraud risk. By its nature, the industry manages the transportation and distribution of goods of all types (usually in large quantities) and oversees high volumes of financial transactions across customers and suppliers each containing multiple stakeholders. In our experience the largest fraud risks predominantly arise from high level managers within the business colluding with other key internal and external players.

In this paper we address what a modern Supply Chain Fraud looks like, what you can do to minimise the risks along with tips to empower you to properly manage the investigation and fraud recovery processes. Whilst it's nice to see the robbers go to gaol, its far healthier for your business bottom line to identify all the key players and maximise your recovery prospects.

Supply Chain Fraud- An Overview

We see the risks of supply chain fraud falling into several groups[1]:

1. Theft and resale of product.This is more prevalent in supply chains for fast moving consumer goods or high demand industry products.If you can't personally use it, sell it or convert it why steal it?
2. Financial fraud via the manipulation of internal/external systems records causing inappropriate payments;
3. Bribery, kickbacks and extortion of key senior managers by third parties.

The fourth category is cyber theft however that is a huge topic too big to cover in this article.

Most businesses are naive to the risk of employee fraud until it is uncovered. Managers place confidence in their Supply Chain & Inventory Management Control Software systems (SCMS) and regular internal auditing to detect aberations and properly track the inventory from receipt to dispatch. There is no doubt as to the power of SCMS and the huge productivity benefits it brings. Yet the statistics, and certainly our experience, have proven that most systems can be easily worked around, particularly when collusion is involved. The KPMG[2] 2016 Global Fraud Survey reports that more than half of the frauds committed were aided by the business' own technology systems:

- 24% of frauds used the business' technology to create false or misleading information in accounting records;
- 20% of frauds used the business technology to provide false or misleading information via email or other messaging platforms;
- 13% of frauds arose where an employee abused permissible access to the business' computer systems;
- 3% of frauds occured by accessing to a business' computer systems without permission;
- 8% of frauds used the business' technology in some other manner[3].

When fraud is uncovered in a business it creates literal shock waves within the business management. Their shock is mostly due to realisation that a senior manager (perhaps their boss or peer) had been a key player in the commission of the fraud. The remaining managers feel a sense of embarrassment, shame, anger, betrayal and worry that their career will be tarnished: "How did you not realise what he/she was doing? Aren't you supposed to check these things?". It's often that these emotions then guide the investigation and recovery process resulting in the process getting rushed, the manager called in and sackedand the supplier agreement terminated. It is all rushed out of fear and the need to show senior management that "action has been taken". Invariably the haste to put out the fire obscures the full truth: all the key collaborators are not revealed and the full value of the fraud may never be known or may only filter out over several months. A rushed investigation allows the surviving collaborators to slowly destroy the remaining eletronic/paper trail and after a while they resign, and thrown a farewell party. Everyone has cake and the collaborator walks away untouched and unknown. As a rule of thumb any fraud that is initially uncovered is just the tip of a very large iceberg.

[1] Supported by IIA, AICPA & ACFE, 'Managing the Business Risk of Fraud: A Practical Guide' (2008)

[2] Global Profiles of the Fraudster, KPMG International, 2016

[3] In addition, the 2016 Deloitte poll (Deloitte, 'Fraud risk assessment: Escalating the battle against supply chain fraud, waste, and abuse' (2016)) found that just under a third of all respondents experienced supply chain fraud, waste or abuse in the previous year.

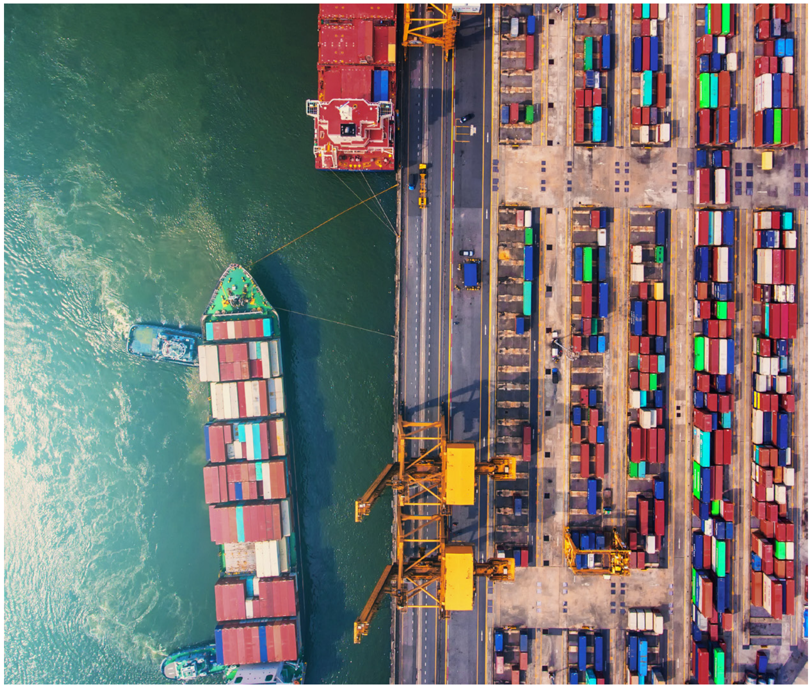
Symptomology of Modern Supply Chain Fraud

The world is changing and so is the manner of workplace fraud. Single player fraud still occurs in organisations, though its mostly confined to shop floor & warehousing workers pocketing product, for example, damaged stock disappearing or inventory falling off the back of the truck. The power of integrated supply chain inventory tracking and inventory control software has taken huge strides in nutting out workers who help themselves to product. It happens but tends to be isolated and low level. You don't see warehouse staff walk out the door with a pallet of product or divert a shipping container of product to their own storage unit without the Company's alarm bells being raised quickly. Lone wolf fraud is more likely to confined to payroll or a finance team with lax controls, such as where accounts payable/receivable is a combined function with little oversight.

The dominant fraud within the manufacturing and logistics industries, both in terms of occurrence and the size of the fraud, occurs through the collusion of staff and also through the collusion of staff and an external supplier/customer. A high level fraud risk assessment of manufacturer/supply chain inventory largely dictates the risk profile of the fraud[4]:

(a) The fraud risk for stock theft is highest for businesses who store and distribute products that are FMCG, high value, high demand or have a modest to high scrap metal value. There is no point stealing boxes of breakfast cereal that cannot be sold on the black market. Unfortunately these business are also exposed to the financial frauds described below.

(b) For other manufacturers/supply chain businesses that do not fit the above profile, the primary fraud risks focus on financial transactions with third parties. Every creditor to a business (which there could be hundreds or thousands) is a potential source of leakage[5]. Supply chain business' are particularly susceptible due to their high transaction volumes. A gentle skim of just 0.1% of a business with an annual turnover $100,000,000 turnover nets $100,000 pa.



[4] See Also Deloitte, 'Fraud Risk Management – Providing Insight into Fraud Prevention, Detection and Response' (2014).

[5] Small businesses are more vulnerable to cyber-attacks etc as they have less security and are more resource-constrained, and can be used to target or provide an 'entry point' to large businesses, especially where the two intersect (ie a small business manufacturer feeding stock into a large business distributor). Tracey Caldwell, 'Securing Small Businesses – The Weakest Link in a Supply Chain?" (2015) 9 Computer Fraud and Security 5, 8.

Collusion is a Genuine Threat

Modern supply chain fraud predominately involves collusion and collaboration between multiple employees, particularly across vertically aligned roles to circumvent business authorisation protocols and checks. Importantly, the digitisation of the workforce and reliance on SCMS leads to circumstances where data & system controls can be bypassed, overridden or authorised and erased. The increase in IT systems has also reduced headcount within organisations and placed greater reliance on individuals and small groups to authorise or investigate aberrations. These staff are typically in a direct vertical reporting structure. The colluding manager signs off the fraud then makes the transaction disappear or otherwise ensures the product never enters the permanent records.

The typical misappropriation of product profile looks like this:

Controller:	Supply Chain Manager/Supervisor who manipulates the electronic records or falsifies/confuses the records.Usually the head of the fraud syndicate and oversees payment to the rest of the group.
Handler:	Warehouse/Logistics Operator manages the receipt, storage and dispatch of the "product". They get a kickback from the Controller.
Get Away Driver:	Third party truck driver collects and dispatches the "product" to an agreed location. In some instances they will deliver the product directly to the black market purchaser. Sometime false invoice records are created with the syndicate's bank account details in lieu of the company to give a veneer of legitimacy.
Fence:	Third Party Fence who receives and on sells the product on the black market and pays the Controller. These are usually only present for high volume theft, unique or hard to dispose of products.

The typical financial transaction fraud is a lot simpler and usually involves potentially two internal staff and at least one external party. They fit the profile of either:

- Kickbacks[6] by the supplier (typically a smaller business owner) to the Senior Manager. In one instance, we've dealt with the Managing Director of a logistic business (who was a dismissed and sued) held a silent 50% ownership of a transport company and used improper influence and inside information to shift their status in a matter of several years from transporting 5% to 95% of the company's outbound freight; OR

- Falsified transactions, refunds and credits within the business records.[7] This allows the Senior Manager to authorise payment (perhaps approved by senior accounts team manager or processed by an accounts payable officer who is part of the syndicate) to the supplier which is then hived off and split within the group.

  This can range from:

  - company payments to transport companies or suppliers for delivering and transporting "phantom" products. The SCMS records are altered to trace the "phantom" product into/out of the business. The resulting misalignment of transported units versus sold units are reconciled via write offs, refunds, discounts or confusing back &forth internal adjustments that make it extremely difficult to reconcile. It is common for a manager to direct his/her staff to make a variety of adjustments to a variety of customer ledgers, "Sales told us to give them a credit- just fix it can you?" This puts distance between the adjustments and the managers own digital finger prints;

  - company payments to suppliers of contractors for services not undertaken: labour hire, cleaners, security guards, gardeners, maintenance workers. The variety of un-provided services is endless.

[6] Usually money, entertainment, gifts and some instances drugs and sexual services (for more information see EY Global Fraud Survey 2016- Justifying Unethical Behaviour & Misconduct). The latter presents a significant risk of a reverse fraud for an organization where the senior manager can be blackmailed by the supplier to provide rate increases, favourable treatment or kickbacks to avert disclosure of their illegal activities.
[7] See also IIA, AICPA & ACFE, 'Managing the Business Risk of Fraud: A Practical Guide' (2008)

What Can You Do?

Acknowledging that fraud has occurred, or is occurring, in your business is never easy, or comfortable. It may bring shame, embarrassment or fear, and it is for these reasons why many managers do not report employee criminal activity to their companies. They may believe that their performance or capability will be brought into question, and potentially threaten their employment. Equally, they may be unwilling to 'dob in' colleagues or friends. Unfortunately but not entirely unexpectedly, this discourse of reluctance only serves to propagate the damage, as these managers become unwittingly complicit in the schemes by failing to reveal the fraud to the company.

Detecting a fraud involving internal/external collusion is difficult but it is possible to narrow the field of potential fraudsters within the business in order to avoid throwing a broad net of auditing with the hope of catching something. We have set out above a basic risk profiling to establish if your business is exposed to financial fraud or product and a financial fraud. There are a number of physical barriers[8] that can be created to minimise individual employee product fraud however collusion based product fraud is harder. However there are a number of things can be done to increase your chance of detecting it:

1. Set up a Whistle blower hotline
   It may sound paranoid but due to the elevated fraud risk of the Supply Chain industry there is some merit to establishing a whistle blower hotline that allows employees to call if they are suspicious. The information gathered from the hotline should be reviewed by no less than 2 managers with diametrically opposed positions in the business to avoid contamination. Your workforce see and hear a lot more than they are given credit for.

2. **Observe staff activity**
   Managers should keep an eye out for suspicious behaviour from staff and other managers, including:
   - excessive personal phone calls during working hours;
   - speaking in code or using cryptic language; and
   - unusual staff interactions, such as a Senior Manager and Forklift Operator regularly engaging in discussions.

   Also of importance are movements in staff morale, including levels of dissent and distrust, which may indicate that some employees have become aware that their colleagues are engaging in duplicitous practices behind the company's back.

3. **Undertake Management Reviews of activities outside audit periods**
   We recommend undertaking functional reviews of a department's operations at random times throughout the year. This should be conducted, where possible, by people outside the function or line of management. Avoid appointing the manager who "volunteers" to do this job.

   Any irregularities from the review, even minor irregularities, should be raised with a tight circle of leaders and external advisers to consider the implications and identify patterns.

[8] Architectural' elements are one of the three requirements for an effective security system (along with technological and operational): Geoffrey Harris, 'Security and Fraud: Strategies for Prevention and Detection' (1991) 4(3) Logistics Information Management 36, 38-39.

4. **Monitor annual leave**
Leave registers should be regularly reviewed to ensure that managers and employees are taking blocks of leave and are not calling in to "help out" when on leave. Manager/employees involved in fraudulent schemes commonly do not take leave for fear of their misconduct being discovered by their replacements.

   For Managers who are department heads, power or ability to alter computer records or authorisation to bypass systems should be directed to regularly take leave in blocks. There will be serious pushback on this, usually citing operational reasons for their need to stay. However a short term operational difficulty is better than large scale fraud.

5. **Treat Spaghetti Like Ledger Adjustments with Suspicion**
If your inventory management records or financial records contain a number of messy adjustments, credits, transfers, errors and/or corrections[9] then this should be a red flag. Junior level incompetence is often blamed but it should be elevated to the whistle blower line or a tight circle of leaders/external advisers to consider investigating.

[9] This is where data analytics comes into its own, especially as the fraudsters get greedier; and it may be able to cross-reference activity with certain time periods, employee access etc. Sunder Gee, 'Fraud and Fraud Detection: A Data Analytics Approach' (2014), 325

Responding and Recovering Losses

Upon unearthing fraud occurring in their business, the instinctive response of many people may be to immediately raise the alarm. As set above, this impulsiveness may alert the perpetrators, allowing them to cover their tracks and hide evidence of any wrongdoing. Therefore, we recommend caution.

If any of the indicators previously explored are triggered, you should stop and consider the likelihood that there are other people within the business who are involved. How high does the fraud go? Who is the appropriate contact to notify? It may be necessary to escalate the matter to the CEO, Managing Director or an Executive that sits outside the operational area in which you suspect the fraud is occuring. If you are still unsure, wait, gather a bit more evidence discretely to help you get a bit more perspective on who are the collaborators. Waiting and watching may seem counter intuitive however very rarely is fraud a one off event.

Fraudsters dont go for one big heist- thats the profile of a criminal sitting outside your organisation. Workplace fraud undoubtedly involves relatively small and repeated thefts. There is usually a distinct pattern to the thefts - they follow the same "winning pattern" of bypassing/ penetrating your systems. The temptation to do it again and again is an extremely strong motivator when it looks like no one suspects anything.

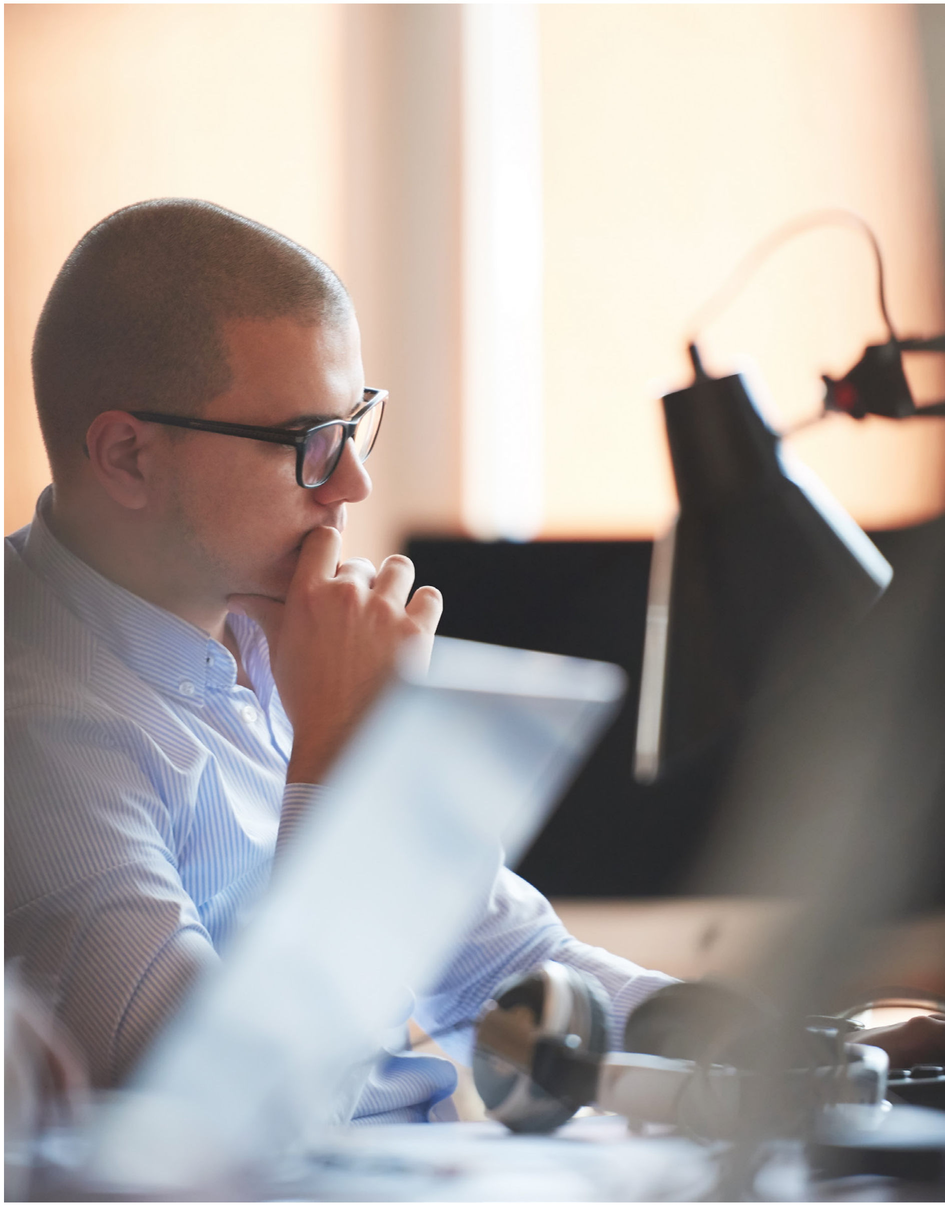
The next step is critical: gather evidence by observing, learning, and recording who is involved, and how they are engaging in the fraud. We strongly recommend:

1. Establish an extremely small team to work on this project, no more than 2 or 3 people to avoid leakage;
2. Engage legal advisors to help you undertake the searches, surveillance and evidence gathering in a lawful manner. We will also advise you on evidentiary gaps to help maximize your recovery abilities.
3. Engage forensic accounting and IT experts to help trace through the transcations to identify the fraud collaborators.

We have successfully lead these investigations on numerous times. It is extremely important to conduct the investigation lawfully and focused on piecing together the money train. Keep your eye on the prize: who has the money? You will undoubtedly gather sufficient evidence to have the employees dismissed, liable for theft and criminally convicted, but your focus should include an attempt to recover the money. Computer systems and messaging can be monitored, mobile devices imaged, staff can be surveilled remotely (careful to do so within lawful means), your stolen product traced to see who are the black market buyers and most importantly to identify where the money trail goes. Where possible try to identify the financial account details, names, BSB & account numbers for any highly suspicious transactions. Out of work hours, you should run systems reports to track similar payments to that account- using the company's most recently backed up data on a terminal set up with your system software but disconnected from the network - **DO NOT USE LIVE SYSTEM DATA** to run diagnostics in case one of the perpetrators are remotely monitoring activities.

We recommend not involving the Police until you have sufficient evidence of the fraud, its players and a plan to persue the recovery. However if at any stage you are concerned that any of your staff (or their family) could be exposed any danager then go directly to the Police and report the matter. Your team's safety must come first. Otherwise we would recommend you involving the Police if you cannot lawfully obtain key evidence, such as covert camera surveillance.

We have repeatedly prepared briefs of evidence for the Police on behalf of our clients and coordinated with the Police as to the investigation status to hasten the process of charges being laid.



Legal Recovery

In our experience the profile of a typical supply chain fraud does not represent a dead end for legal recovery. Due to the profile of the lead fraudsters- senior managers who usually are high net worth individuals with various fixed assets-there are genuine opportunities for the affected companies to take legal action to recover some or all of the value of the stolen products or monies that have been embezzled. Often the lower level players, when confronted with the realisation of bankruptcy, will want to cooperate and assist you in any legal action against the ring leaders.

How can you pursue the money? There are a number of very powerful legal mechanims at our disposal that we can call on to help uncover missing details, stop the flight of money and the destruction of critical evidence. For example once we have a strong prima facie case of the fraud (thanks to the strong investigation we've managed) we can use civil legal processes to apply to the Supreme Court for "pre discovery orders". This allows us to obtain details of the account names (hence Defendant) from a financial institution to where the monies have gone. We can then apply for a Mareva Injunction (a powerful asset freezing order) to effectively freeze those accounts and any other financial institution accounts that are associated with the fraud. The injunction "captures the loot" and stops it being disposed of whilst the legal claim proceeds through the Supreme Court.

Alternatively, if your products have been misappropriated or there is critical evidence that could be destroyed or sent out of the jurisdiction, then it is open to apply to the Supreme Court for "search and seizure" order, referred to as an Anton Pillar order. It is the equivalent of a civil search warrant. All of these orders can be obtained from the Court without the Defendants being tipped off. The first they know about the legal recovery action is when their online banking doesn't work and there's a knock at the front door at 8.00am by a solicitor serving an Order of the Supreme Court to conduct a search. FCB legally supports businesses through these processes, offering practical advice and assistance for navigating the pitfalls. We have strong collaborative relationships with expert forensic IT and forensic accounting businesses.

Not all legal action needs to be that extreme, however we recommend that your strategic goalsremain focused on loss recovery, managing any ASX and public relations implications in the market from the news and patching the hole in your systems through which the fraud was committed.

Conclusion

Regardless of size or location, all businesses in the manufacturing and logistics sectors are at risk of supply chain fraud. It's never too early to start thinking about how to strengthen your processes to reduce this risk- particularly management reviews of critical systems, ensuring staff take leave and establishing a whistle blower hotline. It's equally important for managers to be empowered through trainingto recognising some of the common fraud symptoms and understanding how to respond if you become aware of something fishy.

As Australia's leading workplace relations boutique law firm, FCB Workplace Law, has significant depth of experience in managed a large volume multiplayer workplace frauds. We have assisted countless clients through the difficult stages of responding to fraud tip offs, managing investigations and evidence gathering, urgent Court applications to freeze assets/bank accounts along with coordinating the law enforcement officials and recovering lost assets.

About FCB Group

Founded in 1993, FCB Group is Australia's leading workplace legal and HR solutions business. We deliver strategic advisory services in the areas of employment law, HR management, technology and migration.

FCB is made up of five businesses that fit together like a jigsaw:

- **FCB Workplace Law** - specialist employment law firm;
- **FCB HR** - workplace consulting;
- **FCB Smart Visa** - migration services;
- **enable HR** - cloud technology and solutions; and
- **HR Assured** - a complete workplace solution for small to medium enterprises.

This multidisciplinary approach means we examine workplace relations issues from every angle, so that we come up with the most effective solutions for clients.

About the authors

Matthew Robinson is a partner and solicitor with FCB Workplace Law. Based in our Sydney office, he has been advising clients on industrial relations and employment matters for almost 20 years.

Matthew is an accredited specialist in workplace and employment law. An experienced industrial relations strategist and with a strong skillset in enterprise bargaining, Matthew has special expertise in assisting clients operating in the manufacturing sector.

Would you like to find out more?

If you would like to find out more about how we can help with workplace relations issues in the **manufacturing industry**, please call us on **(02) 9922 5188** or email Matthew Robinson at **mnr@fcbgroup.com.au**.

Ceri Williams

Ceri is a solicitor at FCB Workplace Law. Although based in our Sydney office, Ceri has worked with clients across Australia, including in Victoria, Queensland and South Australia.

During her time at FCB, Ceri has gained valuable experience providing advice to a number of employer associations through a telephone advisory service and bespoke consultancy work.