AURION GUIDE TO FRAUD-PROOF PAYROLL

CONTENTS

PAYROLL FRAUD AND YOUR BUSINESS

Payroll is the largest expense for many organisations, and fraud specifically relating to the theft of cash or sensitive information via payroll systems and tools can be one of the most damaging forms of theft.

Payroll fraud accounts for around 17 percent of money lost to fraud by organisations in Australia. Unfortunately, it's nearly impossible to accurately quantify because so much payroll fraud goes undetected or is not publicly reported. In short, payroll fraud is more common than you might think.

Thankfully there are a number of actions you can take to help ensure the risk of payroll fraud across your business is minimised, including staff education and training, and tightening your payroll processes and systems.

IDENTIFY VULNERABILITIES

Payroll fraud takes many forms and new threats emerge all the time. Some scams exploit weaknesses and blind spots within your business and payroll systems, and some undermine from outside by soliciting personal information to intercept payments – these scams are potentially harder to monitor and control. The key is to know what to look for, and have a payroll system and process designed for transparency and oversight.

Some common types and sources of payroll fraud are outlined here, although this list is not exhaustive.

EXTERNAL THREATS

IMPERSONATION SCAMS

An increasingly popular method of payroll fraud involves external parties accessing employee information through email or 'phishing' scams and redirecting employee funds. These scammers typically send emails impersonating either an employee, a manager or a payroll administrator seeking personal information or to update personal information without authorisation, such as bank account details.

SUPPLIER COLLUSION

Contractors inflate their claim for hours worked or manipulate financial data to receive performance-based bonuses, with or without the assistance of internal staff.

PAYROLL STAFF

ADVANCES NOT PAID BACK

The most passive type of payroll fraud is where an employee requests an advance on their pay and then never repays it. This type of fraud typically happens when payroll staff do not record or monitor advances or repayment efficiently, so appropriate procedures to review advances will eliminate this issue.

GHOST EMPLOYEES

Payroll staff either create a profile for a non-existent employee in the payroll records or prolong the pay of an employee who has just left the company, and redirect fraudulent payments to their own account. This method of payroll fraud is most prevalent in big companies where supervisors have teams so large it's difficult to track compensation in sufficient detail.

PAY RATE ALTERATION

Employees collude with the payroll administrator to increase the amount of their hourly pay in the payroll system. The administrator seeking to avoid detection will often return the pay rate to its original level after committing this fraud for just a few pay periods, so that the issue is less easy to spot. This method of evasion can be detected by matching pay rate authorisation documents to the payroll register.

GENERAL STAFF

BUDDY PUNCHING

Employees punch each other's hours into the company time clock while not physically there to claim un-earned wages. Supervisory reviews and the threat of termination are the best ways to avoid this risk. Another solution is to use biometric time clocks, which uniquely identify each person who is signing in.

UNAUTHORISED HOURS

Perhaps the most common type of payroll fraud is the padding of time sheets by employees, usually in small enough increments to escape the notice of managers. This is a particular problem when managers are known to make only cursory reviews of time sheets, so the best control over this type of fraud is system automation or more rigorous manager review.

"An increasingly popular method of payroll fraud involves external parties accessing employee information through email or 'phishing' scams and redirecting employee funds"

IMPLEMENT PREVENTION STRATEGIES

Preventing payroll fraud requires vigilance from everyone in your business. However, by establishing a few simple processes, supported by education and continual communication, your business can be protected.

"29% of fraud and economic crime in Australia is committed by employees"

PwC 2018 Global Economic Crime & Fraud Survey: Australian Report

COMMUNICATION

- Communicate regularly with the whole business about common scams and methods of payroll fraud – for example, phishing and 'impersonation' email scams.
- Provide a secure, trusted and easy method for your team to contact you if they suspect a scam or fraud incident.

TRAINING

- Securely self-manage or communicate changes to their personal and payroll information.
- Manage passwords, including creating strong passwords and regularly changing these.
- Update all personal and payroll information regularly, to reduce the likelihood of impersonations and other scams.

SYSTEMS

- Create documented processes for managing scam and fraud incidents, so that when you're contacted you are able to respond swiftly and effectively.
- Establish a secure portal for employees to log and send payroll change requests – such as bank account changes – to ensure only registered employees or delegates are able to send payroll changes.
- Undertake regular fraud and security testing, which can include engaging a third party to attempt to breach your security, in order to test your processes and responses.

POLICY

- Develop, communicate and reinforce organisational policy on fraud and dishonest or deceptive behaviour related to payroll and provide a clear escalation procedure for reporting suspected incidents. Your code of conduct (or other policy outlining your expectations of employees) should specifically address payroll fraud and how you will respond to any incidents through disciplinary action or termination.
- Consider implementing a Whistleblower Policy that outlines the obligations and responsibilities of all staff who suspect wrongdoing and provides adequate protections for employees reporting suspected fraud.

"By establishing a few simple processes, supported by education and continual communication, your business can be protected."

Jacqui Birch, Aurion BPOS Client Executive

FRAUD-PROOF YOUR PAYROLL TEAM

Unfortunately, a significant amount of payroll fraud can be enabled by to poor quality or badly implemented processes and tools. The good news is that you can avoid most of the common payroll fraud opportunities with some review and tightening of your payroll management.

TRAINING AND EDUCATION

- Train all payroll staff to identify and monitor for specific anomalies that may indicate fraud. For example, the lack of deductions from a pay record would appear suspicious and may indicate a perpetrator seeking to maximise their gains.
- Provide frequent training and education around privacy legislation and importance of maintaining compliance with privacy legislation in payroll environments.
- Regularly update your team about recent or common payroll phishing scams and prevention.

PAYROLL PROCESSING

- Ensure segregation of duties in the pay processing cycle, separating those who process pay runs from the bank approvers (off cycle and pay run payments).
- Where manual touch points are required for pay runs, then implement, review and update quality assurance processes to align with best practice, such as a quality assurance process for onboarding and separating employees by a payroll employee who is not involved in the initial process.
- Develop an authorised delegation matrix for your organisation, listing who can send payroll requests and aligned by request type, such as hours change, payment of allowances, new hires and separations.

PRE-PAY RUN PROCESS

PRE-PAY RUN CHECKS

- Produce an on (new starters) and off (terminated employees) report within each pay cycle and ensure these records align to the onboarded and terminated requests received from the authorised delegate.
- Audit all changes to employee payroll records, particularly banking information, before completing any payroll activity. Seek confirmation of payroll-impacting changes from the employee directly if this has not been previously provided.
- Perform quality assurance on all variances in pay records, with each variance aligning to a request from an authorised delegate.
- Review any off-cycle payments that were/are due within pay cycle. Sufficient evidence (documentation) should be included detailing what each off-cycle payment relates to.

PRE-PAY RUN AUDIT

- Generate a variance report listing all employees to be paid in each pay run, and the variance from the employees' standard pay outcome. All pay records with a variance are checked and what the variance relates to is noted.
- Produce a trial pay report reflecting current payroll payments before the pay run, and inhibit employee self-service and database access to a limited number of employees (if required at all) to ensure no further changes are made that would impact pay.
- Reconcile the final pay run outcome against pre-pay run reports (step above), and ensure as few changes as possible are made by authorised delegates during the lock-down period.
- Review pay outcome totals by an authorised delegate who provides the approval to run pay.

PAY RUN PROCESS

- Categorise pay-run reconciliation by transaction type – such as gross, tax, net, super, allowance, deductions and superannuation guarantee payments – to monitor fluctuations in pay run totals.
- Match all fluctuations back to change requests from authorised delegates.
- Implement an automated pay-run process to secure and restrict bank file paths. This will mitigate anyone's ability to amend bank files after the pay run, bank portal load and approval.
- Ensure bank approvers have sufficient information, such as reconciliation from pay run, to approve bank portal load. Include approval from the authorised delegate who approved pay run totals during the pre-pay run process.

AUDIT SYSTEM ADMINISTRATION

An important part of preventing payroll fraud lies in having the right payroll systems in place, ensuring that these automate as much as possible to reduce human touch, and keeping systems properly maintained and compliant. With less opportunity to introduce 'holes' into a system, your payroll will be more secure.

SECURITY

- Strictly control access to business systems and information – ensure access to payroll or HRM systems align to individual or group roles and responsibilities.
- Restrict your staff's ability to make payroll changes in employee self-service portal inside work hours, by implementing 'Same Sign On' (enabled by SAML – Security Assertion Markup Language).
- Discuss with your payroll provider adding Multiple Factor Authentication (MFA) to your employee self-service system, in particular changes to bank accounts.

DATABASE GOVERNANCE

EXTERNAL ORGANISATIONS

- Regularly review creditors' (external organisations) codes and inactivate those not recently used. Ensure their accounts have not been changed without official confirmation and communication from the creditor.
- Requests for new codes should come from authorised delegates only and should be accompanied by supporting evidence (documentation). On receipt and entry, the process should be quality checked by another payroll team member.

EMPLOYEE INFORMATION

- Implement an automated workflow with the ability to route and assign activity to authorised personnel, thus minimising human touch points and likelihood of unauthorised actions from unauthorised delegates.
- Implement a process for the ongoing review of system access, roles and responsibilities.
- Establish and implement a clear procedure to ensure ex-employees are removed from database on the day of separation.

Aurion is a pioneer of innovative People & Payroll Solutions. For over 30 years we've been a market leader, helping hundreds of organisations to find simple, effective solutions for their complex People & Payroll challenges.

At Aurion, we work hard to understand your business needs and make your work life easier. Contact us today to find the right solution for your business.

Aurion is part of the Chandler Macleod Group and is a Member of Recruit Holdings Co., Ltd - the 4th largest staffing company in the world.

CHANDLER MACLEOD
UNLEASHING POTENTIAL

RECRUIT

1300 287 466

AURION.COM