The Employer's Guide to Sharing Employee **Income** Information **Securely**

Contents

Foreword

Employers are on the frontline of an imperative to keep their worker's personal information (PI) protected and private. A PricewaterhouseCoopers global survey has found a 17% jump in cyber threats and fraud involving employee data. Fraudsters are targeting human resources and payroll accounts teams with email scams that seek to access employee payroll records to steal personal data like names, bank accounts and tax file numbers.

Employees are also increasingly aware of the need to protect their data. An Office of the Australian Information Commission survey found that 87% of Australians want more control and choice over the collecting and use of their personal information.

As the gatekeepers of employment and employment income PI, employers are responsible for raising the bar in protecting against fraud and identity crime. With nearly half of younger Australians not trusting their employer with how they handle their personal information, forward-thinking employers have an opportunity to reverse this perception.

Be the employer that cares

This guide highlights the main risks inherent in employees' and employers' conventional practices for sharing employment-related PI with third parties. We step you through how the risk environment has changed and why organisations must embrace newer, more secure processes for helping their employees when sharing their employment income information.

We'll also explain what can go right when employers use an award-winning ISO 27001-certified and SOC II certified solution, the Verification Exchange by Equifax. This new model for employment and employment income verification is reshaping the way employee data is shared with third parties while ensuring that Australian Privacy Principles are met.

A triple winner at the Australian Business Awards 2022, the Verification Exchange was recognised for Process Innovation, HR Innovation and New Product Innovation. Its ground-breaking approach removes the need for printed payslips to be part of the accepted behaviour for verifying employment income in Australia.

An employment income verification that, in the past, may have seen the employee download their PI in the form of a payslip and email that to a 3rd party, or upload it to a 3rd party's website, can now be done instantly through the exchange. Payroll data is used as the source of employer verified information in a secure and controlled way to alleviate security and privacy concerns. Its consumer-permissioned approach champions secure and transparent data exchange and is fee-free for employers and employees.

01 - Times have changed

When an employee seeks to reach a life goal, like buying a car or moving onto the property ladder, this begins the process of sharing personal employment and employment income information with a third party. The conventional practice, in a finance context, usually looks something like this:

Sound familiar? You may have a similar process at your workplace or through a payroll provider that does it for you. Either way, it's a process characterised by manual data handling and transmitting personal information over email or phone, each of which is risky and presents unnecessary security risks.

The digital landscape is getting riskier

Do you remember when we used to think it was acceptable to drive a car without a seat belt or use a mobile phone behind the wheel? Over time, we learnt these practices weren't okay, so we changed our behaviour. But at the time, we were blissfully unaware.

The same goes for employment income verification. Our conventional processes may have worked in the past, but times have changed. It's not okay to still use insecure manual processes when the world has become riskier and embraced digitalisation.

Today's threat landscape is very different from what it was just a few years ago. The pandemic has accelerated this metamorphosis. Cybercrime is now a lucrative trade thanks to our increased dependence on the internet and the increased accessibility of criminal activities like ransomware* via the dark web.

**Ransomware* is a type of malware that works by locking up or encrypting files. A ransom is demanded to restore access to the data.*

Understand your market

While it's easy to reject changing an existing process because you think it's secure enough, this is one instance where you need to take a long, hard look at how times have changed in the market.

Instant access requires personal information faster

- Digitisation has improved experiences
- Access to credit is easier
- But requires personal information to be shared faster
- Risk factors increase with open digital sharing

Speed to yes leads to speed to risk

Personal data has become easier to hack

- Before digitisation, opening credit/loan accounts was done with a person at the bank
- Personal information was not as widely or quickly distributed
- Today, it lives in accessible formats that can be compromised

Advanced security protection required

Fraud and ID theft become common

- Online bank accounts can be easily hacked into - data, phishing, scams
- ID crime is one of the most common crimes in Australia
- 1 in 4 victims from ID crime
- Covid-19 pandemic has fueled fraud and identity crime

Data privacy consciousness on the rise

Risky practices belong in the past

In the light of these market changes, do you see how the self-serving and emailing of employment income-related PI is a risky practice that belongs in the past? As an employer and gatekeeper of this information, start asking yourself the same questions that your employees are asking:

- Do I know whom I'm talking to?
- What will be done with this information?
- Who will see and have access to this information?
- How will I share this information safely?
- What can happen when this information is shared unsafely?

Check if you're guilty of any of the following. If you are, it's time to review your processes:

Your team don't consistently check that the people requesting personal information are whom they say they are

You share personal information in a PDF that could easily be hacked or copied

You don't know whether the URL to which personal information is loaded is secure and verified

Staff are not asked for consent to share the specific personal information being released

You're receiving fraudulent emails or calls

Your team has no safeguards in place to guard against manual data error or fraudulent tampering

You can't be sure you haven't made a data entry error when sharing personal information.

You're allowing your employees to 'self-serve' and use your company systems to download their employment income related information and share this with 3rd parties. Have you considered if there are consequences if one of your employees were to have their personal information compromised?

02 - Recognise the stakes are high

Who knew that cybercrime against Australian businesses would escalate to the point where an attack is reported every eight minutes? Or the average financial loss per successful business email compromise* event would leap more than 1.5 times from the previous year.

Many similar metrics show that the cybercrime stakes are getting higher. Unsafe data access and transmission practices can expose personal information to unauthorised third parties. Check out the table below to see what can happen when employee information gets into the wrong hands.

***Business email compromise** is a form of phishing where criminals use emails to pretend to be business representatives to trick organisations into sharing PI.

What can go wrong?

Below are some conventional practices and the risks they pose

Self-serve downloading of payslips - tampering

- Payslips can be falsified to overstate income to lenders.
- According to a bank survey, 37% of borrowers make misrepresentations on their loan applications.
- Employer processes may be perceived as facilitating fraud

Self-serve downloading of payslips - unauthorised access

- Payslips can be printed, scanned, or emailed by a person posing as your employee.
- False accounts can be created in employee's name or personal information sold to criminals.
- According to PwC's Global Economic and Crime Survey, 43% of respondents have experienced fraud from an external perpetrator and 31% from a threat actor within their organisation.
- Data is not encrypted or protected during email transfer or personal delivery.
- No control over how the end user receives and manages the data.

Answering verification phone calls

- Without an adequate screening process, the employer doesn't know if the person calling to verify an employee's income is who they say they are.
- HR/payroll might accidentally miscommunicate information about an employee that impacts the employee's loan application, or disclose more personal information than is legitimately required.
- Taking time to ensure consent is in place for sharing the precise, relevant personal information lengthens the application process.

Emailing or uploading payslips to a 3rd party website

- Employer's staff can receive phishing*, scam emails or calls and be tricked into disclosing PI to fraudsters.
- Employers might accidentally send inaccurate information that impacts an employee's loan application, or disclose more personal information than is legitimately required.
- Employers risk sending information to non-verified sites where it could be stolen.
- Employers have no visibility over where the PI is stored once sent.

Sending PDFs

- Hackers or internal threat actors can intercept a PDF, even if it has been password protected.
- Employers might accidentally send inaccurate information that impacts an employee's loan application, or disclose more personal information than is legitimately required.
- PDFs can be tampered with by the sender to falsify information.

*Phishing is when cybercriminals masquerade organisations to access sensitive information.

What's at stake?

IMPACT ON EMPLOYEES

If your employees find out early enough that they've been a victim of identity theft, they can have new cards issued, and passwords reset. But find out too late, and the impact can be huge. Their savings could be stolen, bills racked up in their name, and fake loans taken out – all causing an emotional and financial toll that can take years to recover from.

REPUTATIONAL RISKS FOR YOUR COMPANY

Employees expect you to keep their data safe, so a cyber incident represents a significant breach of your employee's trust and confidence. With data breaches often plastered in the news headlines, companies can experience substantial reputational damage and longer-term difficulties in attracting talent and building loyalty.

COMPROMISED EMAILS

The inherent security weakness of email makes it a favourite tool for hackers to spy on personal data. When information leaves your inbox, it passes through multiple servers, leaving it vulnerable to attack as it makes its way to the recipient's inbox. Hackers are keen to collect this kind of data to sell on the dark web or to facilitate identity theft and financial fraud. While good security practices can help protect emails, they can't altogether eliminate the risk.

PHONE SCAMS

Some phone scams (like robocalls) are easy to spot, but fraudsters impersonating a bank or employer are harder to detect. Scammers who trick people into giving out information like full name, income, date of birth or address can use this data to fill out false applications for loans or commit other forms of fraud.

EMPLOYEE CONSENT

There are many grey areas regarding what personal employee information organisations can disclose to a third party under data protection laws. The Fair Work Ombudsman recommends the best practice approach of asking for your employee's consent each time you disclose personal information about them.

EMPLOYER LIABILITY

Where internal privacy-compliant processes are inadequate or do not exist, there is an increased risk that the employer will be held vicariously liable for any privacy breaches of the employee, including inadvertent disclosures.

Employers who do not have processes in place for securing PI and enabling its safe sharing are potentially in breach of the Australian Privacy Act. This risk will only grow with proposed reforms to the employee records exemption, increased regulatory penalties for non-compliance and a right to sue for breach of privacy being considered as part of the Federal Government's next tranche of privacy reforms.

CASE STUDY:

The Australian Information Commissioner ordered an Australian employer to pay $60,000 in damages to 14 employees for breaching their privacy with unauthorised data disclosures. The privacy training, privacy access controls, procedures and policies of the business were found to be inadequate. This case highlights the potential privacy risks employers might face when failing to protect personal information.

03 - Mitigate the risk - Equifax Verification Exchange®

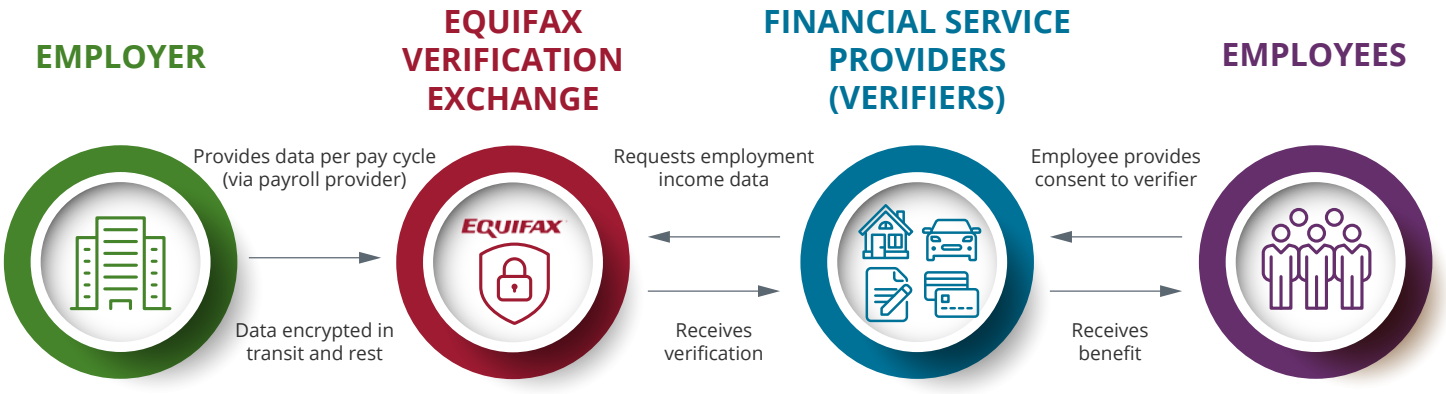
Do you see how alarmingly easy it is for your conventional processes to open up risks to your business?

So let's consider what you can do as an employer to mitigate these risk

Take an automated, hands-off approach

If there's one thing you can do to protect your business, it's to remove your involvement in the process. Yes, that's right – as an employer, you can step away from your hands-on approach to sharing an employee's employment income information. Instead, your employees and their financial service providers can access payroll data from source rather than through copies of payslips

Employers can do this by allowing payroll data to link to the innovative 'digital vault' that is Verification Exchange. The data is 'linked' securely, with information being encrypted and only shared with a credentialed financial service or other provider when the employee's consent has been given.



- Real-time accurate Income and Employment information shared
- Automated process with no manual steps
- Consent driven process for authorised and credentialed lenders / brokers only
- Speed to decision making significantly reduced

Here's how we make it happen:

Mitigating the risk for employers

No longer open to the dangers of printing, scanning and emailing, personal information data is only accessible by a credentialed verifier with the employees' consent. Verification Exchange mitigates the risk by:

Removing the perils of manual handling

- ✓ No more manual data handling
- ✓ No risky print/scan/email/phone data transmission
- ✓ No sharing of unsecured documents.

Providing a secured pathway to transmit data

- ✓ Employee provides consent each time to initiate the process
- ✓ Verifiers must supply a permissible purpose
- ✓ Verifiers have their identity credentialed under stringent requirements imposed by Equifax as Australia's largest facilitator of data brokerage services
- ✓ Reduces risk of employer being held vicariously liable for privacy breaches and inadvertent disclosures
- ✓ We check and verify relevant requests, emails and websites used by the Verifiers.

Replacing manual handling with secure, automated reports

- ✓ Standardised reports with only relevant personal information
- ✓ Aligned with STP (Single Touch Payroll) reporting
- ✓ Direct feed of payroll data
- ✓ Encrypted and secured consumer data reports
- ✓ A complete picture of individual employment and three-year pay history

Ensuring best practice data security management

- ✓ Aligned to Australian Privacy Principles
- ✓ Complies with Australia's privacy and data protection regulations
- ✓ ISO27001 certified
- ✓ SOC 2 Type II certified
- ✓ Incorporates security measures that include encryption, tokenisation and stringent identification requirements.
- ✓ Data stored and processed in Australia
- ✓ Incorporates globally recognised best practices in data security management
- ✓ Equifax is an industry leader in data security, with security capabilities ranked in the Gartner top 1% of analysed technology and financial service companies.

Want a deeper dive into the security and compliance environment we employ for Verification Exchange? View or download "Our Philosophy Towards Security" and our "Security Annual Report" here.

Verification Exchange is a fee-free service

As a final benefit, there is no charge to an employer for using the Verification Exchange. It's also a fee-free service for your employees. Credentialed verifiers, such as financial service providers, pay a fee to receive employment income information directly from Verification Exchange – but only when your employee consents.

04 - Lead with best practice

Good data governance and data protection are becoming increasingly essential to executive leadership and corporate success. Building a culture of data privacy and cybersecurity now, rather than waiting on legal actions and regulatory penalties, shows your employees, customers and the broader community that your company acts with integrity

Work place health & safety

Compliance with Australian privacy principles

Employers can lead a new frontier in digital employee safety. Even when not required by law, this layer will ramp up privacy and security, providing confidence and assurance.

It's time to be..

- ✓ Secure
- ✓ Pro-active
- ✓ Certain
- ✓ Leader in charge
- ✓ Forward thinking
- ✓ Best in class
- ✓ Gold standard of safety
- ✓ Guardian
- ✓ Data custodian
- ✓ Overly protective
- ✓ An organisation that does the right thing

It's not okay to be..

- × Complacent
- × Not aware
- × Ignorant
- × Not up to speed
- × Sub-par
- × Apathetic

Give your employees control and choice

87% of Australians want more control and choice over their personal information.

With Verification Exchange, your employees have complete oversight. A third party cannot access their payroll records without first seeking their one-time consent.

Furthermore, your employees have the option to place a block on their data directly with the Verification Exchange so that it cannot be shared at all.

Give your employees confidence and trust that when they need it, their information is being shared safely and securely.

59% of Australians have experienced problems with how their personal data has been handled. Employees expect to be able to access and understand how their data is being used and disclosed.

Verification Exchange provides data exchange transparency, which is essential to building trust. The amount of payroll data shared with the third party is limited in accordance with the instructions of the employee to whom it relates.

Give your employees protection against identity fraud

The top two privacy concerns Australians have are identity theft/fraud and data security/ breaches. Employees want their personal information protected against inadvertent disclosure.

With Verification Exchange, payroll records are stored in a high-security digital vault only to be accessed by credential verifiers with a valid purpose and the employee's consent. This removes the risk of inadvertently giving out employee details to a fraudulent third party.

Give your employees confidence in the quality of data

41% of data breaches are caused by human error, the most common being emailing personal information to the wrong recipient. Manual data handling processes are prone to human error, especially if the information derives from multiple sources, such as different payroll and HR systems.

Verification Exchange uses payroll data as the source of verified information, eliminating any risks of data entry errors. Since payroll data contains the most accurate and detailed record of an individual's employment income, Verification Exchange provides a single source of truth for identifying and verifying an individual's employment status and employment income across potentially multiple employers.

05 - Elevate your digital duty of care

As an employer, we know you take the care of your employees seriously. You value their safety and protection above all else. In a digitised world, their safety extends to data security.

Show that you are a secure and safe employer that cares by joining the employers and payroll providers around Australia already contributing payroll records to Verification Exchange.

Proposed Changes to Australia's Privacy Laws

Employers who do not have processes to secure personal employee data and enable safe sharing risk breaching the Australian Privacy Act 1988(Cth). The risk of class actions, increased penalties and liability to pay compensation will only grow with proposed reforms such as:

- Removal of the employee records exemption, requiring employers to apply privacy principles to employee records.
- A right to sue for breach of privacy.
- Employers to meet baseline security requirements as 'reasonable steps' to ensure a secure method of PI data storage and transfer.

Protecting your employees with a higher level of care

Do the right thing by your employees. Good workplace privacy and data sharing practices can set your business up as a trustworthy custodian of your employee's data, protecting against the legal and reputational repercussions of unauthorised access or misuse of personal information.

The Fair Work Ombudsmen advises that best practice employers choose to tell employees:

- what personal information they collect
- why they are doing so
- who they might pass that information on to
- how they can access their own personal information
- how to verify or correct their personal information if it is incorrect, outdated, or incomplete, even when not required by law.

The Verification Exchange is a practical way to exercise your duty of care.

Demonstrates high standards of digital citizenship

Helps protects sensitive data from fraud and unauthorised use

Data is securely stored and managed in Australia within the exchange

Is transparent with how personal employee information is stored and shared

Employee consent is required to initiate any dealings

Controls access to confidential information

Limits the amount of information divulged

Helps employees move more quickly to achieve their major life goals.

Hopefully, this guide will make you think twice about allowing your employees to continue to print, email and upload payslips to verify their employment income.

Remember, Verification Exchange can help you become a better employer by:

- Moving with the times
- Recognising the stakes are higher
- Mitigating the risk
- Leading with best practice
- Elevating your digital duty of care

Contact us to find out how to start contributing your payroll data to this FEE-FREE, award-winning, innovative employment and employment income verification solution.

We do it all for you - we source the relevant income data, obtain employee consent, and create data reports for the employee that remove the risk from you.

Go with Equifax Verification Exchange®

EQUIFAX