InPayTech
Integrated Payment Technologies Limited

# DATA SECURITY

## Does your SuperStream and STP process protect or expose you to data breaches?

**Integrated Payment Technologies**

In the age of 'big data', organisations have the opportunity to harness the power of information, but also the obligation to protect what data they have in the face of constant threats.

This is true for businesses of all sizes, since even the smallest business cannot operate without generating data on its employees, suppliers and customers. The complexity and volume of data is growing exponentially.

The data explosion extends to the payments system, where transactions are increasingly being made through digital means, including internet banking transfers, digital credit cards and other online payments systems such as PayPal.

Data security is therefore vital, especially in the finance sector, where a huge amount of personal information is kept and transmitted by employers to organisations including banks, superannuation funds and government bodies such as the Australian Taxation Office (ATO). This includes data about employees' salaries, superannuation contributions, ages, addresses and other personal information.

A recent study by global market intelligence firm IDC titled *Data Age 2025* predicts that worldwide data creation will grow to an enormous 175 zettabytes (ZB) by 2025. That's ten times the amount of data produced in 2017. Yet data from new sources will raise new risks of breaches to private and sensitive information according to the IDC study. By 2025, almost 90 per cent of all data created will require some level of security, but less than half will actually be secured.

This exposes organisations to huge risks. Data breaches can result in confidential details such as a person's address or salary details becoming publicly available. Reputations can be seriously damaged when privacy is breached, as we saw with Facebook's involvement in the Cambridge Analytica scandal in 2018. Facebook is still trying to manage the additional scrutiny this scandal has raised. Organisations need to take strict measures to ensure the security of their data, particularly customers' and employees' personal and financial information.

This white paper will explore options all superannuation and payroll organisations can use to implement payment related data systems that meet the strict requirements being imposed by the Australian Taxation Office (ATO).

Organisations which stick with the status quo and continue to transfer data via unsecure locations face a much greater risk of a data breach due to human error or a malicious cyber-attack, which can greatly harm their reputations.

## Responsibility on employers, payroll providers and super funds

Employers, payroll providers and super funds, as recipients, retainers and transmitters of a huge amount of personal information, have a very high level of responsibility for ensuring their data transfers are secure because things can, and do, go wrong.

In the recent past, the personal information of several hundred members, from a large fund, was leaked by a senior fund employee. This resulted in significant legal costs and reputational damage to the super fund. Just last year, the accounts of about 11,000 members, from another large fund, were the target of a data security breach. While the fund took immediate action when the breach was detected, there were concerns the personal details of its members, including names and addresses, were compromised. The fund was in the news, as it often is, but this time for the wrong reason. This will happen to organisations that fail to fully protect data appropriately.

Eligible data breaches are now notifiable and may trigger severe sanctions. The Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) amends the Privacy Act 1988 (Cth) to introduce mandatory 'eligible data breach' notification provisions for organisations regulated by the Privacy Act. These regulated entities include super funds.

Eligible data breaches must be reported to the Office of the Australian Information Commissioner (OAIC) and recent statistics show that many of the entities reporting breaches are in the finance sector. The Notifiable Data Breaches Quarterly Statistics Report: 1 October – 31 December 2018 reveals that the OAIC received 262 notifications from 1 October to 31 December 2018, compared to 242 from 1 April to 30 June 2018.

**The type of personal information most commonly involved in data breaches was contact information, followed by financial details and identity information. All these types of information are kept and transmitted by employers and super funds in the SuperStream process.**

Overall, malicious or criminal attacks accounted for 168 data breaches in the last quarter of 2018, or 64 per cent of the total, while human error accounted for 85 data breaches, or 33 per cent. System faults accounted for just nine data breaches, or 3 per cent.

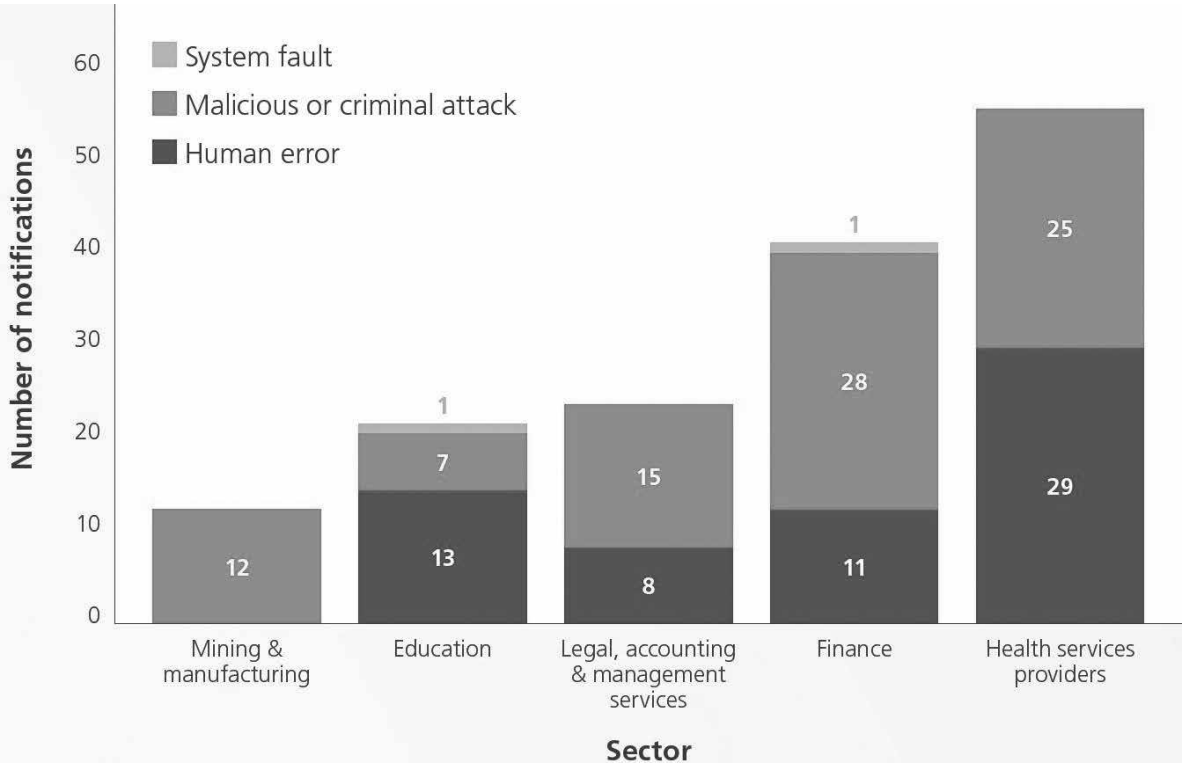
Human error included sending personal information to the wrong recipient via email (27 per cent) or mail (12 per cent) as well as unintended release or publication of personal information (18 per cent).

Other types of human error were the loss of paperwork and the loss of a data storage device.

Within the finance sector, there were 40 notifications to the OAIC. Of these, 27 per cent were caused by human error while the bulk (70 per cent) was the result of malicious or criminal attacks. Of these attacks, cyber incidents were the most common (57 per cent), followed by rogue employees or insider threats (25 per cent), social engineering/impersonation (11 per cent) and theft of paperwork or a data storage device (7 per cent).

What this shows is that payments systems must be able to sustain

**Figure 1. Source of data breaches – Top five sectors**




*Source: Office of the Australian Information Commissioner (OAIC), Notifiable Data Breaches Quarterly Statistics Report: 1 October - 31 December 2018*

their integrity in the face of cyber-attacks, as well as be immune to human error.

Figure 1 breaks down the sources of data breaches by notifying entities in the top five sectors, including finance.

## How your data could be at risk

Many employers today utilise a portal process to send SuperStream data to superannuation funds, as per Figure 2.

Data is downloaded from a secure payroll system and onto a desktop and then uploaded to a secure portal for transmission to superannuation funds and the ATO.

And herein lies the risk: with data being downloaded onto a desktop or shared drive, it is potentially exposed to malicious or criminal attacks, or human error – the leading causes of data breaches in Australia.

## How to protect your data

One of the most common forms of data protection is encryption. Building encryption into online platforms and software has been a critical approach for elevating privacy and protecting sensitive data without depending on the weakest link – people – to protect the data.

Any encryption system must meet the 'Confidentiality, Integrity and Availability' standard. In the world of superannuation contributions, where the volume of personal and financial data is growing exponentially, this is truer than in any other field.

Beyond encryption, safe storage is crucial to protecting data as more and more data is retained by organisations and transmitted electronically. The OAIC report shows that the loss of a data storage device and theft of data from a data storage device are not uncommon causes of notifiable data breaches, so organisations need to take precautions against such risks.

The introduction of single touch payroll (STP) requires the ATO to be notified of Pay as You Go (PAYG) tax deductions and the pay details of every employee.

The ATO will only accept STP messages from secure 'whitelisted' STP providers referred to as digital service providers (DSPs). All DSPs who use the ATO's digital services such as STP need to meet the ATOs requirements, which include:

- Authentication
- Encryption
- Supply chain visibility
- Certification
- Data hosting
- Personnel security
- Encryption key management
- Security monitoring practices.

## A secure, encrypted process

To help protect employees' data from cybersecurity risks, DSPs should provide superannuation funds, employers and payroll providers with a secure API to prevent personal and private data from being exported outside of a secure business management system.

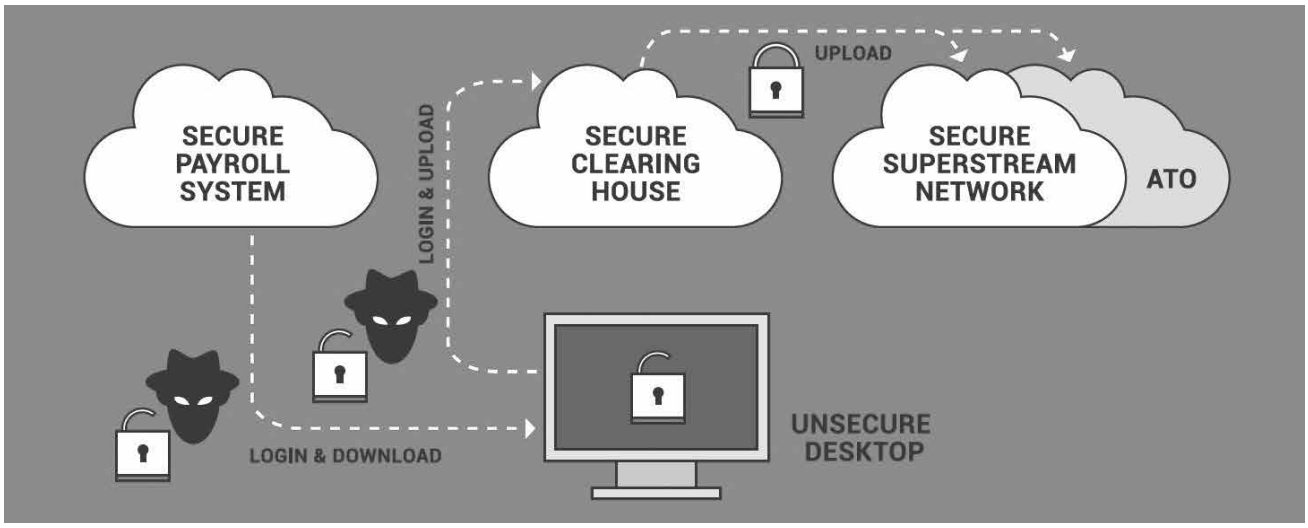
Users can log in to the payroll system and data is sent from the DSP platform through a secure connection.

A DSP should process STPs directly to the ATO and sends SuperStream data files to the superannuation funds via the SuperStream network. All personal and financial data should be sent via a secure data centre. Data should never be loaded onto a user's desktop or shared drive outside of the password protected system.

This helps to defend against the number one source of notifiable data breaches: malicious and criminal attacks. It also helps to minimise human error, including the unauthorised disclosure of data, the loss of data stored on a desktop or mobile device, and the loss of data contained in paperwork.

Moreover, the physical security of the data stored in data centres extends far beyond the office environment. Data centres should be protected by firewalls and the data must be 'encrypted at rest', which means it is not stored in 'plain text' on a disk drive, as it often is on a user's desktop.

**Figure 2. Data at risk of attack**



Our clearing house solution ClickSuper meets all ATO requirements and boasts core competencies in delivering highly secure, automated and compliant payment and message handling services, including STP data transfers to the ATO and superannuation contributions distributed using the SuperStream network.

It has physical, organisational, administrative and electronic security measures in place to reduce the risks of loss, misuse, unauthorised access, disclosure or alteration of information.

A summary of the security measures include:

- Access authorisation controls;
- Firewalls, virus scanning software and anti-intruder systems;
- Use of secure networks or data encryption when users receive or send personal information electronically;
- Restriction of access to information to staff who require it to perform their job function;
- Instructing staff on the obligations relating to handling of personal information;
- Physical access controls to data centres; and
- All data transfers are made through Hypertext Transfer Protocol Secure (HTTPS), which is used for secure communication over the Internet, and the communication protocol is encrypted using the highly secure version of Transport Layer Security (TLS1.2). This dramatically reduces the risk of data security breaches and identity theft. Identity crime is one of the most common crimes in Australia. The estimated direct and indirect cost of identity crime in Australia in 2015–16 totalled $2.65 billion, according to Australian Institute of Criminology's report *Identity crime and misuse in Australia 2017*. This includes $2.1 billion in losses suffered by Australian government agencies, businesses and individuals.

Another key benefit is the ability to make same-day superannuation contribution payments to employees' accounts. This avoids the need for monies to be held for three days by superannuation clearing houses, during which time it is sitting idle and not earning a return.

## Conclusion

As the age of big data rolls on and organisations accumulate more and more information, they need to be more vigilant about data security, particularly in light of the ever-present threat of cyber-attacks and another weak link in the chain, people.

DSPs should provide superannuation funds, employers and payroll providers with a payment data transfer service that sits within a secure API to prevent personal and private data from being accessed. The solution should avoid the need for organisations to export data outside a secure business management system and instead retain personal data and financial information inside the secure 'plumbing' of the SuperStream and Single Touch Payroll processes. **FS**

**Figure 3. Securing and encrypting data**