

Byfields Newsletter

February / March 2019



Welcome to the new year!

Each year, before diving into our long list of projects, we look back at what worked well the previous year, what we achieved and what can be improved. It's a valuable process that puts us in the position of being very present in the new year. We hope you have a similar ritual that works to ground you, to have you acknowledge what you did achieve, and to set you up for the year.

Contents

Denying Deductions for Non-Compliant Payments	1
4 Year Time Limit on GST Refunds	2
R&D Tax Incentive	2
Travel Smart with Cyber Security Tips ..	4
Key ATO Dates for February 2019 & March 2019	5

Denying Deductions for Non-Compliant Payments

The Treasury Laws Amendment (Black Economy Taskforce Measures No 2) Bill 2018 received Royal Assent on 29 November 2018. Schedule 1 of the Bill will disallow a taxpayer from claiming an income tax deduction for certain payments where the required withholding obligations were not complied with. The Bill applies from 1 July 2019.

The proposed section 26-105 would affect the following payments:

- Payments to employees;
- Payments to directors;
- Payments to religious practitioners;
- Payments under a labour hire arrangement;
- Payments for a service where no ABN has been quoted.

While the new rules are aimed at denying deductions for so called "cashies", it is important to note that the amendment also captures non-cash benefits provided in-lieu of a cash payment. In both cases, a deduction will also be

denied for payments where the obligation to withhold was made but not notified to the Australian Taxation Office (ATO).

Where a taxpayer withheld an incorrect amount and has notified the ATO, a deduction will still be available. The ATO provides an opportunity for taxpayers to correct any contraventions made provided an amount has been withheld, and a notification has been made. The amendment appears to primarily target total failures to withhold.

The ATO recognises that there are situations where an employer honestly believes their employees are acting as contractors even where this position is not upheld by the ATO. In these circumstances, the proposed amendment does not deny a deduction to the taxpayer provided the taxpayer has appropriately withheld payments made to the "employee".

The introduction of this measure goes hand-in-hand with the expected mandatory adoption of Single Touch Payroll (STP) for all employers from 1 July 2019. Legislation to extend STP to employers with 19 or fewer employees is currently before Parliament, and once it has received Royal Assent, same-day reporting for wages and director fees will be mandated for every employer in Australia.

Disclaimer: The information contained in this newsletter is provided as a guide to the general public and, whilst the content is believed to be accurate, no liability is accepted for any errors or omissions. Recipients should contact Byfields before acting on any recommendations and cannot place any reliance on such recommendations without this contact.

4 Year Time Limit on GST Refunds

On 23 November 2018 the Commissioner issued Draft Miscellaneous Taxation Ruling MT 2018/D1 'Miscellaneous tax: time limits for claiming and input tax or fuel tax credit'.

This ruling seeks to clarify the Commissioner's literal approach to the operation of the 4 year limitation period on claiming input tax credits (ITCs) in the GST Act and on claiming fuel tax credits (FTCs) under the Fuel Tax Act. Under this approach, regardless of whether you have requested the Commissioner amend your assessment, applied for a private ruling or object to an assessment, your entitlement to claim ITCs expires if you have not claimed the ITCs or FTCs in your activity statement within 4 years.

The Commissioner's somewhat controversial view of the words "taken into account in an assessment" is taken to mean that an entity must include the claim for ITCs or FTCs in the calculation of the net amount or fuel tax amount. Thus under this view, unless an entity claims the ITC or FTC within 4 years, their entitlement expires.

This fundamentally differs from the pre-self-assessment regime in place before 1 July 2012, where an entity could lodge a notification under s 105-55 of Schedule 1 to the TAA to protect its entitlement to claim ITCs without being exposed to penalties and interest.

Under the Commissioner's literal approach, taxpayers can only protect their entitlement to an unclaimed ITCs or FTCs by actually claiming those credits in an activity statement. This will expose taxpayers to penalties and interest if the claim is subsequently determined to be incorrect.



Thus, if this ruling is adopted, taxpayers who determine that they may have an entitlement to recover ITCs/FTCs face the decision of whether to:

- claim the credits in their activity statement (thereby exposing themselves to penalties and interest if the claim is incorrect); or
- engage with the Commissioner to recover those credits by:
 - * requesting an amendment to an assessment; or
 - * apply for a private ruling; or
 - * objecting to an assessment.

If Commissioner engagement is chosen, taxpayers must expect that the process will be completed within the 4 years. If not – even if the delay is the fault of the Commissioner – or the delay is as the result of various appeal processes through the Courts (which turn out to be successful for the taxpayer), a taxpayer's entitlement to ITCs/FTCs expires.

Comments on the ruling were due by 25 January 2019. However clients that believe they are entitled to either ITCs or FTCs for prior years, need to seek advice as to how they can protect their rights in respect to claiming those prior credits.

R&D Tax Incentive

The R&D Tax Incentive is the government's primary program to encourage business research and development (R&D), and registrations for R&D activity conducted during the year ended 30 June 2018 are open until April.

About the R&D Tax Incentive:

To be eligible for R&D Tax Incentives your business must:

- Incur eligible R&D Expenditure through a company structure;
- Conduct experimental activity where the outcome cannot be determined in advance;
- Generate new knowledge by developing new or improved:
 - * Products;
 - * Processes; or
 - * Services.

Companies engaged in R&D may be eligible for the following tax benefit:

- Where group turnover is less than \$20 million, a 43.5% refundable tax offset provides the following for eligible expenditure depending on a company's tax position:
 - * a 43.5% cash refund to the extent a company is in tax loss;
 - * a 16% tax saving/refund if a company is in a tax payable position.
- Where group turnover exceeds \$20 million, a 38.5% non-refundable tax offset provides an 8.5% tax saving for eligible expenditure.

Important compliance information for companies already claiming the R&D Tax Incentive:

Companies already registering their R&D Activity should be aware of current compliance focuses by program administrators.

AusIndustry and the ATO regularly release new guidance material outlining compliance requirements which should be reviewed during claim collation. Current areas of focus include:

- Research before R&D Activity commences to show knowledge generated did not exist;
- Substantiation of the process and results of experiments conducted during the R&D Activity;
- Substantiation of the time claimed for personnel conducting the R&D Activity.

Proposed Changes to R&D Tax Incentive announced in May 2018 Federal Budget:

Changes were announced to the R&D Tax Incentive in the May 2018 Federal Budget which included:

- Changes to R&D Tax Offset rates:
 - * Where group turnover is less than \$20 million, the refundable R&D Offset is proposed to be based on a company's tax rate + 13.5%;
 - * Where group turnover exceeds \$20 million, the non-refundable R&D Offset is proposed to be based on a progressive rate determined by the company's R&D 'intensity';
- Changes to caps on R&D Tax Offsets for very large claims;
- Changes to other administrative provisions of the program.

While the changes were scheduled to apply for the year ended 30 June 2019, legislation to enact the changes is yet to be introduced to parliament.

Recent events, including the consultation process on the R&D amendments explanatory memorandum and the scrapping of proposed company tax cuts, may impact when, and to what degree the proposed changes are applied.

If you would like to review the eligibility requirements further or discuss your existing claims, please contact our office. More information is also available here:

<https://www.business.gov.au/assistance/research-and-development-tax-incentive>

<https://www.swansonreed.com.au/>



Travel Smart with Cyber Security Tips

The practice of good cybersecurity habits should not be limited to the home or office. It is equally important to implement best practices for a secure computer for safe online behavior and to secure our internet-enabled mobile devices whenever we travel. The more we access the internet when traveling, the more cyber risk we face. No one is exempt from the threats of cybercrime, at home or on the go.

Travelling Tips

Before You Leave:

Update your mobile software

Just like your home or work computers, mobile devices should be routinely updated to prevent security vulnerabilities. By simply applying software and application updates you will greatly improve your devices ability to defend against malware and other threats.

Back up your information

It is good practice to keep a backup of all your devices. This includes stored contacts, photos, videos or any important information stored on your mobile devices. Consider backing up your data to another electronic device, such as a USB, or using a cloud service.

Keep it locked

Get into the habit of using strong passwords or other forms of locking your devices when you are not using them. Even if you are simply stepping away for a few minutes. A few minutes is all it takes for a thief to steal or destroy your information. When possible enable two-factor authentication (2FA) on your devices and online accounts.



While You Are There:

Stop auto connecting

Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or car infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.

Think before you connect

Before you connect to any public wireless hotspot – like on a plane or in an airport, hotel, train/bus station or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network. Only use sites that begin with “https://” when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Think before you click

Use caution when downloading or clicking on any unknown links. Delete emails that are suspicious or are from unknown sources. Review and understand the details of an application before installing.

Guard your mobile devices

To prevent theft and unauthorised access or loss of sensitive information, never leave your mobile devices – including any USB or external storage devices – unattended in a public place. Keep your devices secured in taxis, at airports, on planes, and in your hotel room.

Common Cybersecurity Threats while Travelling

Unsecured wireless networks

While public wireless networks provide great convenience, allowing people to connect to the Internet from almost anywhere, they are unsecure and can allow cyber criminals access to your Internet-enabled devices. Beyond the typical public wireless networks found at airports, restaurants, hotels, and cafes,

they are increasingly available in other places, such as on planes and in public parks.



Publicly accessible computers

Hotel business centres, libraries, and cyber cafes provide computers that anyone can use. However, travelers cannot trust that these computers are secure. They may not be running the latest operating systems or have updated anti-virus software. Cyber criminals may have infected these machines with malicious viruses or install malicious software.

Physical theft of devices

Thieves often target travelers. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If you are attending a conference or trade

show, be especially wary — these venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.

Key ATO Dates for February & March 2019

FEBRUARY

January monthly BAS due (payment and lodgement)	21 February
December quarter BAS due (payment and lodgement)	28 February
December quarter PAYG instalment due (payment and lodgement (if varying the instalment amount))	28 February
Annual GST return or Annual GST information report (lodgement and payment (if required))	28 February
Income tax lodgement and payment for medium to large companies (new registrations)	28 February
Income tax lodgment for medium to large trusts that were non-taxable in the latest year lodged unless required earlier	28 February

MARCH

February monthly BAS due	21 March
--------------------------	----------

For a full list of ATO due dates, go to www.ato.gov.au/Business/Reports-and-returns/Due-dates-for-lodging-and-paying/Due-dates-by-month/.

