enspira financial
enabling aspirations

client alert
tax news | views | clues

Get ready for tax time 2024

The end of the financial year is fast approaching and with that, tax time 2024 is kicking into gear. As it has in previous years, the ATO has recently flagged some primary areas where taxpayers frequently make mistakes on their tax returns. “These are the areas that people are most likely to get wrong”, ATO Assistant Commissioner Rob Thomson has said, “and while these mistakes are often genuine, sometimes they are deliberate. Take the time to get your return right.”

For 2024, the ATO’s vigilance is particularly focused on incorrect claims of work-related expenses, inflated rental property claims, and the omission of income from tax returns. In the previous year, over eight million individuals claimed work-related deductions, with a significant number related to home office expenses. With the revision of the fixed rate method for calculating home office deductions, the ATO now requires more comprehensive records to substantiate claims.

The ATO also reiterates the three golden rules for claiming any work-related expenses: you must have spent the money yourself without receiving reimbursement, the expense must be directly related to earning your income, and you must have a record, typically a receipt, to prove the expense.

Rental property owners are also under scrutiny this year, with data revealing that nine out of 10 are incorrectly completing their income tax returns. The ATO is paying close attention to deductions claimed for property repairs and maintenance, which are often mistaken for capital improvements. While immediate deductions are permissible for general repairs, such as replacing broken windows or damaged carpets, capital improvements like kitchen renovations are instead only deductible over time as capital works.

The ATO encourages rental property owners to meticulously review your records before lodging your tax return, and to ensure that your claims are accurate and backed up with documentation.

The last main area of focus is the timing of tax return lodgments. The ATO firmly warns against lodging your tax return at the earliest possibility (on 1 July), as this can often lead to errors, particularly in failing to include all sources of income. According to the ATO, taxpayers who lodge in early July will be doubling their chances of having their tax returns flagged as incorrect by the ATO. Most income information, such as interest from banks, dividend income and government payments, will be pre-filled in returns by the end of July, simplifying the process and reducing the likelihood of mistakes.

ATO crypto data-matching program extended

Hot on the heels of reports that a growing number of self managed super funds (SMSFs) are sustaining significant losses in crypto asset investments, the ATO has announced it will be extending its current crypto asset data-matching program for the 2023–2024 financial year through to the 2025–2026 financial year. Under this program, identification data will be collected from both individuals and non-individuals, such as SMSFs or other entities.

It is expected that around 700,000 to 1.2 million individuals and entities will be affected in each financial year of the data-matching program. A point of difference with this particular program is that the data retention period will be seven years from the receipt of the final instalment of verified data files from data providers, as opposed to the usual five years for other data-matching programs run by the ATO.

The ATO justifies this longer retention period by pointing to the need to conduct longer-term trend analysis and risk profiling of the crypto market, as well noting that crypto assets are often retained over many years before they are disposed of and trigger a CGT event.

The ATO will use the data obtained from the program to promote voluntary compliance and educate individuals and businesses that may be failing to meet their registration and/or lodgment obligations. In addition, insights from the data will be used to develop compliance profiles of individuals and businesses and initiate compliance action as appropriate.

Navigating complexities of crypto investments: SMSFs

The digital currency landscape continues to be treacherous terrain for self managed superannuation fund (SMSF) trustees, with a growing number of reports indicating significant losses due to a variety of factors, including scams, theft and collapsed trading platforms. The ATO is urging trustees to educate themselves on the potential pitfalls of crypto investing, including the fact that many crypto assets are not classified as financial products. This means that the platforms facilitating their trade often lack regulation, increasing the risk of loss without recourse.

The ATO has identified several causes of crypto investment losses:

- Some trustees are being duped by fraudulent crypto exchanges, which promise high returns but are designed to siphon off investors' funds.
- Cybercriminals are increasingly targeting crypto accounts, hacking into them to steal valuable cryptocurrencies.
- A number of crypto trading platforms, particularly those based overseas, have collapsed, leaving investors with significant losses.
- Some trustees find themselves permanently locked out of their crypto accounts due to forgotten passwords, losing access to their investments.
- Scammers impersonating ATO officials are tricking some individuals into revealing wallet details under the guise of investigating tax evasion, leading to losses.

The ATO is urging trustees to educate themselves on the potential pitfalls of crypto investing. Resources such as the ACCC's Scamwatch and ASIC's MoneySmart provide valuable information on recognising and avoiding scams.

The ATO highlights that many crypto assets are not classified as financial products, meaning that the platforms facilitating their trade often lack regulation. This increases the risk of loss without recourse.

It is important to note that while some may still consider cryptocurrency to be private and anonymous, and may baulk at reporting any gains they've made, the reality is quite different. The ATO has the ability to track cryptocurrency transactions through electronic trails, in particular where it intersects with the real world. In addition, through data-matching protocols, the ATO requires cryptocurrency exchanges to furnish them with information on transactions, making it possible to trace and tax crypto trades. Trustees are therefore encouraged to report all transactions.

For SMSFs that run businesses and accept cryptocurrency as payment, the approach to accounting is akin to dealing with any other asset: the value of the cryptocurrency needs to be recorded in Australian dollars as a part of the business' ordinary income. Where business items are purchased using crypto, including trading stock, a deduction is allowed based on the market value of the item acquired. SMSFs that run businesses should also be aware that there may be GST issues when transacting in crypto.

Superannuation switching schemes and investment scams: what to look out for

Beware of "cold callers" offering to switch your super

Following an extensive review, ASIC has uncovered a worrying trend where cold callers, after procuring personal details from third-party data brokers or through online baiting techniques, have been aggressively pushing consumers to switch their superannuation funds. These cold callers have been found collecting the details of people who use certain online comparison websites, or running competitions for prizes such as phones or gift cards and subsequently misusing the entrants' details.These operations often have ties to a minority of unethical financial advisers who then suggest moving the consumers' funds into superannuation products that carry hefty fees.

ASIC has expressed particular concern about these practices, noting that individuals aged between 25 and 50 – typically the primary targets of these operations – are at risk of significant retirement savings depletion due to reduced super value from unsuitable investments and excessive fees and other charges.

In addition, ASIC has observed a substantial flow of super savings into high-risk property managed investment schemes. These schemes are either channelled through super products offered by Australian Prudential Regulation Authority (APRA) regulated funds or self managed super funds (SMSFs), with subsequent kickbacks going to the cold calling entities.

ASIC has reiterated its commitment to safeguarding consumers, and is urging financial advice licensees and superannuation trustees to intensify their efforts in rooting out the nefarious elements that are targeting people's super. ASIC will continue to take appropriate action, including enforcement action, to deter cold calling.

To raise public awareness, the regulator has launched a campaign advising consumers to hang up on cold callers and scroll past social media click bait offers to compare and switch super funds.

ASIC notes that a typical super cold calling experience does involve receiving a statement of advice (SOA) prepared by a financial advice firm – often one that the cold caller has an existing arrangement with – but it is usually "cookie cutter" advice that is expensive, unnecessary and does not consider a consumer's individual needs, and may eventually leave the individual in a worse financial position. It reminds consumers that quality financial advice takes weeks, not days, to prepare.

Consumers who believe they have received financial advice that was not appropriate for their circumstances can initiate a complaints process, which includes contacting the business that gave the advice, then contacting the Australian Financial Complaints Authority (AFCA). Consumers who believe they have been a part of a scam should report it to their super fund at the first instance, as well as reporting it to Scamwatch and ASIC.

Bond and term deposit scams on the rise

ASIC is also concerned about the recent increase in sophisticated scams that encourage people to invest in fake bonds and term deposits. These scams are particularly insidious as they involve the impersonation of legitimate financial services businesses, many of which may not have a significant online presence of their own.

According to ASIC, scammers have been meticulously mirroring the details of real businesses, including their addresses, Australian business numbers (ABNs) and Australian financial services (AFS) license numbers. These elements are being used in scam advertisements and communications to lend an air of authenticity to the fraudulent schemes.

The scammers' strategy involves using online advertisements and social media posts to lure consumers with fake offers to invest in well-known companies. These ads and posts often redirect to an online enquiry form designed to harvest personal information. Consumers who show interest are provided with counterfeit investment materials and disclosure documents that appear professional and convincing.

ASIC has noted that these scammers are particularly cunning, often presenting themselves as knowledgeable and personable without pressuring potential victims into making quick decisions. The returns advertised are also crafted to sound reasonable, avoiding the typical "too good to be true" offers that are easier to spot as fraudulent.

Once they have gained the trust of their targets, scammers request personal identity documents and the completion of application forms. They then direct consumers to transfer funds into bank accounts that, while seemingly legitimate, are actually controlled by the scammers. These accounts are often held by reputable banks that are not associated with the supposed investment opportunity, further complicating the detection of the scam.

It's important to remember that legitimate financial services businesses are required to hold client money for investments in a trust account, client segregated account or cash management trust that is held in the name of the licensee. ASIC also notes that consumers can confirm bank account details (including whether the bank account details match the name of the financial services business) via the Australian Payments Network or by independently contacting the bank directly using the details on the Australian Financial Complaints Authority (AFCA) website.

People who may have fallen victim to this type of scam are urged to contact their banks immediately and not to send any further money. If you're concerned your ID may have been compromised, you can contact IDCARE, a free government-funded service which can help develop individualised response plans. ASIC advises that these scams should also be reported to Scamwatch to help stop scammers from entrapping more people, and that you should always be wary of follow-up scams that may promise to "get your money back".