QUT Centre for Justice Briefing Paper

ISSN 2652-5828 (Print), 2652-6441 (Online) February 2022 / Issue No 21

Editorial Introduction

Fraud is defined as using lying, cheating and deception to gain a financial advantage. There are many categories of fraud. The Australian Competition and Consumer Commission (ACCC) monitors a range of fraudulent activities through its ScamWatch portal. Individuals are encouraged to self-report experiences of fraudulent activity to ScamWatch to assist the ACCC to monitor trends and identify ways of disrupting identified scams.

One of the key categories of fraud monitored by the ACCC relates to jobs and employment scams, otherwise known as recruitment fraud. Recruitment fraud uses the guise of a genuine job opportunity to lure potential victims to directly pay fees or to share sensitive personal information, such as driver's licence, bank account or passport details. Victims of employment scams expose themselves to a range of consequences, including fraud, identity theft and money laundering.

This briefing paper analyses data sourced from the ScamWatch Jobs and Employment Scams Statistics to identify trends in recruitment fraud in Australia.

Key Trends in Employment Scams in Australia

What are the Gaps in Knowledge about Recruitment Fraud?

Deanna Grant-Smith, Alicia Feldman and Cassandra Cross

Employment fraud can be understood in two distinct ways. In its broader context, employment fraud often centres on employers as the victim and jobseekers as the perpetrator of the fraud. In this scenario, fraudulent candidates seek to defraud a potential employer by lying or providing misleading information about their employment history or qualifications or about another aspect of themselves (Gee et al., 2019). However, employment fraud can also be perpetrated against an individual seeking employment (Beals et al., 2015). For this reason, the term recruitment fraud can provide a useful point of distinction between scams focused on defrauding organisations and those focused on jobseekers.

Within the broad practice of recruitment fraud, there appear to be two distinct sub-genres. The first is primarily associated with labour trafficking, where vulnerable individuals are duped into forced or illegal labour arrangements, such as commercial sexual exploitation in a foreign country (Volodko et al., 2020), or acting as money mules under the guise of being employed as money transfer agents (Esoimeme, 2020). The second type of recruitment fraud occurs when individuals are defrauded into providing money, banking details or other personal information for a job that does not exist (Mahbub & Pardede, 2018). Research is lacking on this second type of recruitment fraud, which is the focus of this paper.

Presenting data sourced from the Australian Competition and Consumer Commission's (ACCC) Scam Watch Jobs and Employment Scams Statistics, this briefing paper explores the current state of knowledge regarding recruitment fraud in Australia. 'Employment scam' is the ACCC's preferred term for describing recruitment fraud, no doubt due to its simplicity and colloquial appeal. However, we prefer the term 'recruitment fraud' to better capture the nature of the offence and the seriousness associated with victimisation. Throughout this paper, both terms are used where applicable to refer to the same broad concept.

Primary Modes of Recruitment Fraud in Australia

Several approaches are used by offenders to perpetrate recruitment fraud. Some seek to harvest personal information from potential employees through posting fake job advertisements that attract individuals to apply and upload sensitive information, which is sold by offenders to a variety of legitimate and illegitimate groups (Vidros et al., 2016). Another approach involves the same ruse to obtain sensitive and personal information about potential employees. However, in this instance, the offenders themselves seek to use this approach to perpetrate identity crime against the unsuspecting victim. Documents sought by offenders include social security numbers, identity cards, passports and bank account information. In this way, offenders can take on the identity of the victim or use their bank accounts to launder funds (Vidros et al., 2017).

Finally, offenders may create fake advertisements and require upfront payments from potential candidates to either cover services or fees related to the potential job or to pay for materials required for the role (Beals et al., 2015).

Examples of this include expenses associated with visas, training, travel or the purchase of starter kits (Mahbub & Perdede, 2018).

A variation to this approach sees offenders pay victims with counterfeit cheques and ask for the overpayment to be transferred back to the offender. Once the cheque is identified as counterfeit, the victim will have to bear the costs associated with the full cheque amount and any amount withdrawn (Beals et al., 2015).

Several recent studies have focused on 'online recruitment fraud' (Mehbook & Malik, 2021; Vidros et al., 2017). However, while such nomenclature recognises the predominantly online nature of this offence, recruitment fraud occurs in both online and offline environments (Cross, 2019).

Table 1 compares the top five modes of employment scams in Australia in terms of their percentage of the total number of reports and the total amount lost. This data shows that while email is the most common mode of employment scam in terms of both numbers of reports and amount lost, in-person scams ranked second highest in the total amount lost for the period 2018–2020.

Table 1. *Top Five Modes of Employment Scam as a Percentage of All Reports, 2018–2020.*

	Number of Reports	Amount Lost
1	Email (59%)	Email (40%)
2	Phone (13%)	In person (28%)
3	Internet (8%)	Internet (12%)
4	Text message (8%)	Phone (10%)
5	Social networking (6%)	Social networking (5%)

Figure 1 shows a higher level of variance in losses by mode (on the right) than in the number of reports by mode (on the left) from 2018–2020. It also highlights the disproportionately high losses for in-person employment scams relative to reports for this same period. By contrast, the number of reports of text message scams is considerably higher than the reported amount lost relative to other scams. No available data identifies whether the reported recruitment fraud is the result of targeted (e.g., jobs listing) or untargeted (e.g., spam) approaches (McCoy et al., 2016).

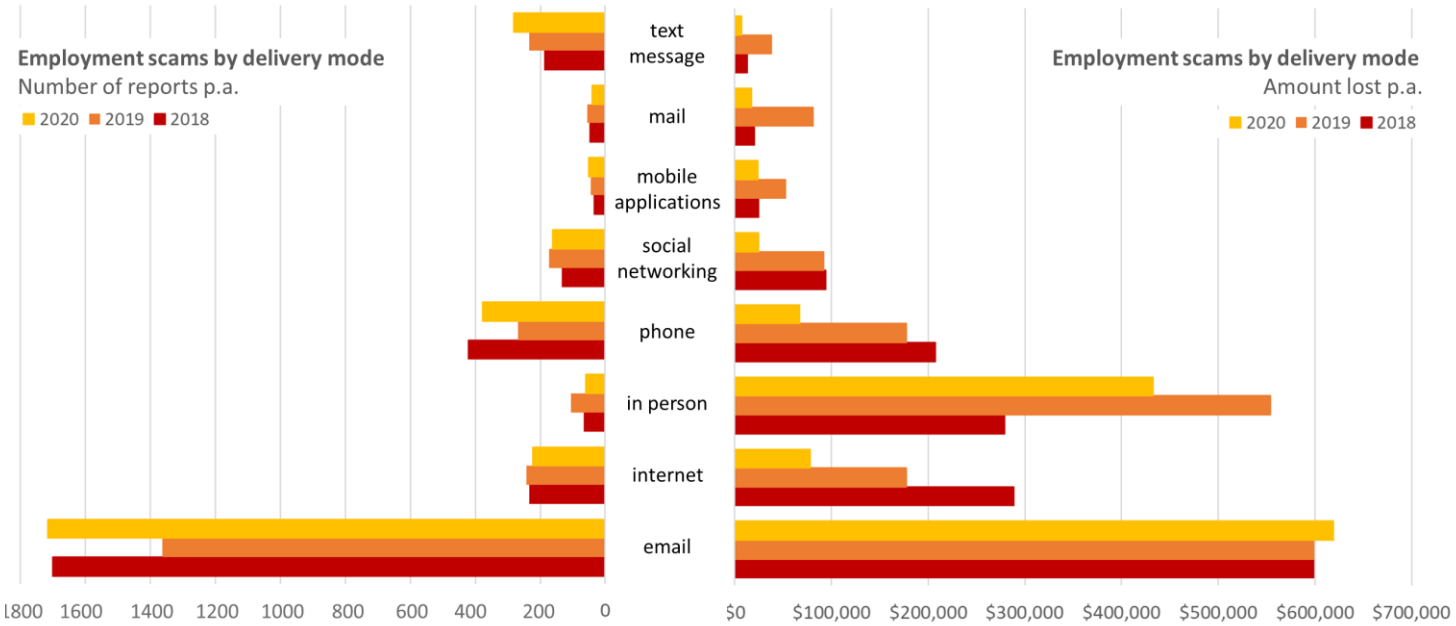

Figure 1. *Amount Lost in Australian Dollars and Number of Reports of Employment Scams per Annum, 2018–2020.*

Prevalence of Recruitment Fraud in Australia

Measures of recruitment fraud rely on the accuracy of individuals' self-reporting, the reliability of their recollections and their willingness to share victimisation experiences. As a result, current data likely underestimate the prevalence and effect of recruitment fraud (Deevy et al., 2012). Estimates are also affected by a combination of under-reporting and under-admitting due to a range of factors, including a lack of recognition that an individual has been defrauded; emotions of shame, embarrassment or self-blame; low financial loss; and confusion regarding reporting and redress regimes (Button et al., 2009).

No study on the prevalence of recruitment fraud in Australia has been conducted.

The ScamWatch data presented in Figure 2 shows clear peaks and troughs in both reports and the amount lost. However, the available data does not appear to reveal any observable seasonal variation, and there does not appear to be any observable connection between the amount lost and the number of reports at a given time.

Profile of Recruitment Fraud Victims

There is no single profile of a victim recruitment fraud. Figure 3 shows reports and losses due to employment scams by victim age for 2018–2020. Unsurprisingly, reports are highest in cohorts representing the working-age population of individuals who are mostly already in or aspiring to join or rejoin the workforce. While reports by age group are reasonably consistent across years, there is not a similar consistency for the amount lost.

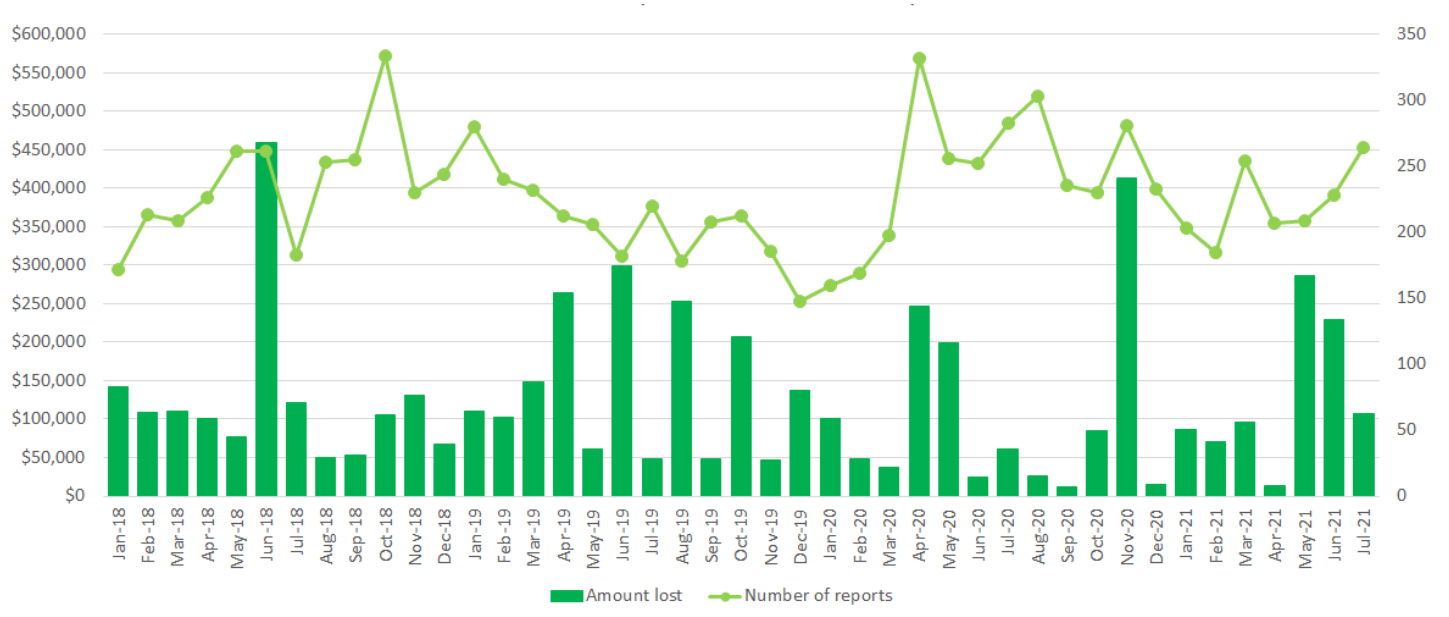

Figure 2. *Monthly Number of Reports of and the Amount Lost to Employment Scams, January 2018 – July 2021.*

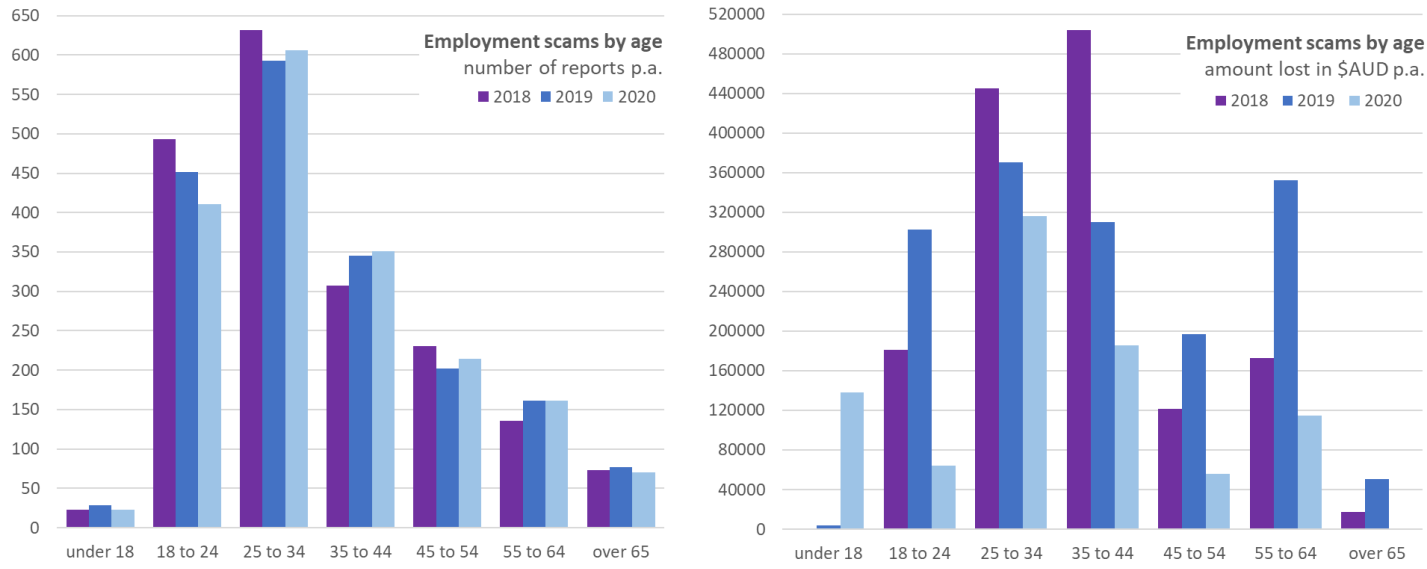

Figure 3. *Number of Reports of and Amount Lost to Employment Scams by Victim Age per Annum, 2018–2020.*

Figure 4 shows that although men reported fewer scams than women in 2018–2020, they also reported greater total losses. There are several reasons this may be the case. Perhaps women are targeted more often and, therefore, are reporting more scams, but they do not fall victim to these scams as often as men. Another explanation is that the workforce participation rate for men is higher (Australian Bureau of Statistics, 2021) and that they might, therefore, be more likely to be targets of recruitment fraud but choose not to report scams unless they lose a large amount.

Yet another interpretation is because it is not necessary to lose money to report to ScamWatch, those who choose to report may not be doing it for themselves but, rather, acting in the hopes of preventing others from experiencing similar fraud (Cross et al., 2016), and there may be gendered differences associated with this altruistic act. Or perhaps this data is truly representative and simply suggests that men have fewer experiences of employment scams but lose considerably more per instance.

It is important to note that the data used by ScamWatch is generated through self-reporting, resulting in a very limited understanding of how well this data represents the actual number of scams and dollars lost by Australians. Overall, each of these possible interpretations provides a clear impetus to explore this difference in further detail.

What the Figures Don't Tell Us

Victims of fraud more generally face challenges in accessing justice through the fraud justice network of police, consumer protection organisations and banks (Button et al., 2013). However, those targeted by employment schemes are often less visible and might, therefore, be more marginalised than those who experience other types of fraud victimisation. Recruitment fraud has the potential to compromise jobseekers' privacy and result in financial losses.

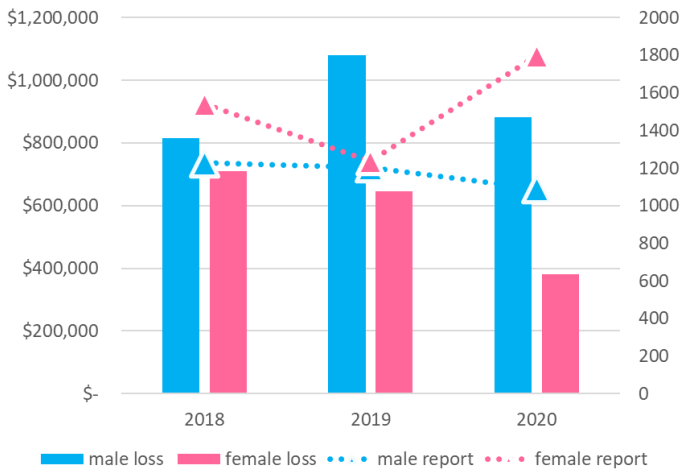

Figure 4. *Number of Reports of and Amount Lost to Employment Scams by Victim Gender, 2018–2020.*

However, the effects of fraud go far beyond this and can result in significant psychological and reputational damage for individuals, particularly given that some who share their experiences of fraud face stigmatisation and ridicule (Button et al., 2009). Indeed, the very characterisation of jobs and employment scams as 'trick[ing] you into handing over your money by offering you a "guaranteed" way to make fast money or a high-paying job for little effort' (Australian Competition & Consumer Commission, 2021, para. 1) can paint the victims of recruitment fraud not only as complicit in their victimisation but responsible for it due to avarice and folly. This degree of victim blaming is not unique to recruitment fraud (Cross, 2015).

Recruitment fraud has the potential to negatively affect the credibility of organisations inadvertently involved in perpetrating such deceptions. Employers can be misrepresented, while employment agencies and job-posting platforms can unwittingly promote fraudulent jobs. However, it can be difficult for individuals and employment agencies to determine if a job advertisement is genuine or fake as there can be few observable differences. This phenomenon has been more pronounced since the beginning of the COVID-19 pandemic in early 2020 and the shift to flexible working arrangements and working from home (Beck & Hensher, 2021), perks that were previously noted as common characteristics of false advertisements (Vidros et al., 2017).

Advancing a Recruitment Fraud Research Agenda

While this paper has focused on the Australian experience, recruitment fraud is a global problem. For instance, between December 2019 and May 2020, over 13,000 job listing scams were reported to the Better Business Bureau's BBB Scam Tracker, which monitors recruitment fraud in Canada and the United States (Stahl, 2020).

Given the ubiquity and global nature of recruitment fraud, research is required on several fronts. First, research is required that accurately quantifies the prevalence of recruitment fraud both in terms of fraudulent advertisements and victims falling prey to such deception.

Second, because assumptions cannot be made about the victims of various forms of cyber fraud (Whitty, 2020), research is necessary to understand the characteristics of those most susceptible to recruitment fraud so that targeted awareness materials can be developed and regional differences identified.

Finally, research that explores the important monitoring and detection role of job placement and posting sites is needed to minimise the posting of fraudulent advertisements and to safeguard sites' integrity.

References

Australian Bureau of Statistics. (2021). *Labour force, Australia, detailed.* www.abs.gov.au/statistics/labour/employment-and-unemployment/labour-force-australia-detailed/latest-release

Australian Competition and Consumer Commission. (2021). *Scam Watch: Jobs and employment scams.* www.scamwatch.gov.au/types-of-scams/jobs-employment/jobs-employment-scams

Beals, M., deLeima, M. & Deevy, M. (2015). *Framework for a taxonomy of fraud.* Financial Fraud Research Centre, Stanford Center on Longevity.

Beck, M. & Hensher, D. (2021). Australia 6 months after COVID-19 restrictions part 2: The impact of working from home. *Transport Policy.* https://doi.org/10.1016/j.tranpol.2021.06.005

Button, M., Lewis, C. & Tapley, J. (2009). *Fraud typologies and the victims of fraud: Literature review.* National Fraud Authority.

Button, M., Lewis, C. & Tapley, J. (2013). The 'fraud justice network' and the infrastructure of support for the individual fraud victims in England and Wales. *Criminology & Criminal Justice*, 13(1), 37–61.

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy & Practice*, 5(2), 120–131.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187–204.

Cross, C., Richards, K. & Smith, R. (2016). *The reporting experiences and support needs of victims of online fraud.* Trends & Issues in Crime and Criminal Justice, no. 518. Australian Institute of Criminology. www.aic.gov.au/publications/tandi/tandi518

Deevy, M., Lucich, S. & Beals, M. (2012). *Scams, schemes and swindles: A review of consumer financial fraud research.* Financial Fraud Research Center, Stanford Center on Longevity.

Esoimeme, E. E. (2020). Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules. *Journal of Money Laundering Control*, 24(1), 201–212.

Gee, J., Button, M., Wang, V., Blackbourn, D. & Shepherd, D. (2019). *The real cost of recruitment fraud*. Crowe and University of Portsmith.

Mahbub, S. & Pardede, E. (2018). Using contextual features for online recruitment fraud detection. In B. Andersson, B. Johansson, S. Carlsson, C. Barry, M. Lang, H. Linger & C. Schneider (Eds.), *Designing Digitalization*. Lund University.

McCoy, D., Park, Y., Shi, E. & Jakobsson, M. (2016). Identifying scams and trends. In M. Jakobsson (Eds.), *Understanding Social Engineering Based Scams* (pp. 7–19). Springer.

Mehboob, A. & Malik, M. S. I. (2021). Smart fraud detection framework for job recruitments. *Arabian Journal for Science & Engineering*, 46(4), 3067–3078.

Stahl, A. (2020, 11 May). Job hunting scams amid COVID-19 pandemic. *Forbes*. https://www.forbes.com/sites/ashleystahl/2020/05/11/job-hunting-scams-amid-covid-19-pandemic/?sh=1e9751a73c57

Vidros, S., Kolias, C. & Kambourakis, G. (2016), Online recruitment services: Another playground for fraudsters. *Computer Fraud Security*, 2016(3), 8–13.

Vidros, S., Kolias, C., Kambourakis, G. & Akoglu, L. (2017). Automatic detection of online recruitment frauds: Characteristics, methods, and a public dataset. *Future Internet*, 9(1), 6.

Volodko, A., Cocknain, E. & Kleinberg, B. (2020). 'Spotting the signs' of trafficking recruitment online: Exploring the characteristics of advertisements targeted at migrant job-seekers. *Trends in Organised Crime*, 23, 7–35.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy & Research*, 26(3), 399–409.

About the Authors

Associate Professor Deanna Grant-Smith, QUT Centre for Decent Work & Industry
Alicia Feldman, PhD student, QUT Centre for Decent Work & Industry
Associate Professor Cassandra Cross, QUT School of Justice

Centre for Justice Briefing Papers are a publication of QUT's Centre for Justice.
They are published through a process of open peer review. The views expressed in this paper are those of the author(s) and do not necessarily represent those of the Centre or QUT.

qutc4j@qut.edu.au
@CrimeJusticeQUT
www.qut.edu.au/law/research/centre-for-justice