# Recruitment Fraud: Increased opportunities for exploitation in times of uncertainty?

Cassandra Cross and Deanna Grant-Smith

*Recruitment fraud uses the guise of a genuine job opportunity to lure potential victims into paying 'fees' directly or sending sensitive personal information (driver's licence, bank account details, passports, etc.). Those who comply can expose themselves to a range of consequences, including fraud, identity theft and money laundering. Victims of fraud more generally face challenges in accessing justice through the fraud justice network of police, consumer protection organisations and banks. However, those targeted by employment schemes are often less visible and might be more marginalised than those who experience other fraud victimisation. In 2020, the emergence of COVID-19 plunged the world into an extraordinary level of uncertainty. Millions found themselves unemployed or underemployed due to the lockdowns and physical distancing restrictions introduced to control the virus, creating a bountiful environment for offenders to effectively target potential victims of recruitment fraud and increasing the vulnerability of a larger proportion of society to such schemes. This article details the contours of recruitment fraud. The paper advocates a research agenda promoting a better understanding of fraud victimisation in this context. Ways to effectively disrupt or prevent fraud are outlined to reduce levels of victimisation and harm into the future.*

KEYWORDS: Recruitment fraud, technology and fraud, fraud victimisation

## Introduction

The evolution of technology continues to drive innovation and change across all aspects of society, including job seeking. A wide range of internet and social media platforms have been adapted to connect recruiters with job seekers, fundamentally altering the ways potential employees are targeted and recruited by employers (Kim et al., 2021). Job seekers choose to engage with potential employment opportunities in very different ways (Baum and Kabst 2014). Residual user concerns regarding perceived privacy risks and information accuracy remain (Petre et al., 2016). However, e-recruitment systems reduce recruitment costs, increase the ability to reach a wider candidate pool, reduce time to hire through greater efficiencies and improve company brand image (Alghamdi and Alharby 2019; Niharika Reddy, Mamatha and Balaram 2019). Unfortunately, offenders also use these platforms for malicious and criminal intent, including labour trafficking (Volodko, Cockbain and Kleinberg 2020) and fraud (Lal et al. 2019).

Fraud can be understood as 'any crime that uses deception as its principal modus operandi' (Button and Gee 2013: 8). Fraud is characterised by lying, cheating (Fletcher 2007) and leveraging deception for financial advantage through various means, including direct money transfers and the harvesting of personal credentials to enable identity crime (Button and Cross 2017). Recruitment fraud can compromise job seekers' privacy and result in financial losses. It can also negatively affect the credibility of organisations inadvertently involved in perpetrating such deceptions, such as misrepresented employment agencies and job-posting platforms that unwittingly promote fraudulent jobs (Vidros et al. 2017).

Based on a reading of the limited current literature, there appear to be two distinct types of recruitment fraud. The first is labour trafficking, where vulnerable individuals are duped into a forced or illegal labour arrangement. Young women are often targeted for modern slavery and commercial sexual exploitation in a foreign country (Mukhlis 2021; Volodko et al. 2020), while young adults and employed individuals may be recruited as money mules under the guise of being employed as money transfer agents (Esoimeme 2020). The second type of recruitment fraud sees individuals targeted to access bank details and personal information, usually for a non-existent job. This second type of fraud is the focus of this paper. Recruitment fraud of this kind, although under-researched, is increasingly relevant in the current times of global uncertainty.

Fraud perpetrators are extremely adept at taking advantage of opportunities and exploiting financial instability and economic and other fears. The COVID-19 pandemic, which emerged in 2020, has led to unprecedented, large-scale lockdowns, social distancing and physical restrictions on the movement of citizens worldwide. Responses aimed at limiting related morbidity and mortality rates have contributed to the loss of employment for millions globally. Ongoing uncertainty for workers due to snap lockdowns and worsening employment precariousness has resulted in massive unemployment and experiences of loss and fear (Blustein and Guarino 2020). However, while emerging studies document a reduction in crimes in public spaces and outside of households during this time (Buil-Gil et al. 2021a; Nivette et al. 2021), there appears to be a corresponding rise in the types and prevalence of offences that occur online (Buil-Gil et al. 2021b). Many fraud categories (Kemp et al. 2021) are tailored specifically to fears associated with the virus (Payne 2020). A growing body of research seeks to explore fraud, how it is perpetrated and its effects on victims (Button et al. 2009; Button and Cross 2017; Cross 2019b). However, there is a dearth of research focused explicitly on recruitment fraud.

This article explores recruitment fraud as a crime category in and of itself, as well as its relationship to COVID-19. Doing so gives visibility to the challenges in raising awareness of specific fraud types and fraud victims attempting to access response to their victimisation through the ‘fraud justice network’ (Button et al. 2013). After providing a definition and overview of recruitment fraud, the article then turns to means of detecting the presence of recruitment fraud before examining its estimated prevalence. The article concludes by advocating a research agenda for providing critical attention to recruitment fraud to reduce the potential harm incurred by victims in the future.

## Understanding Recruitment Fraud

Fraud is premised upon deception for financial advantage. Fraud has existed for centuries (Yar and Steinmetz 2019). However, the evolution of technology has substantially altered the ways offenders perpetrate fraud offences and has exponentially increased the pool of potential targets (Button and Cross 2017). The virtual realm has radically transformed fraud, and offenders have embraced the ease, anonymity and jurisdictional issues experienced by police agencies worldwide (Cross 2019b). In this way, most fraud offenders knowingly act with impunity, leaving fraud victims without any sense of closure or justice (Cross et al. 2016).

Different types of fraud can be defined based on a combination of communication methods (online or face to face), strategy/approach, targeted groups and whether the fraud is committed against an individual or an organisation (Beals et al., 2015). Acts of fraud perpetrated against employers need to be differentiated from those perpetrated against individuals. However, the current terminology does not always allow for this. Two distinct forms of employment fraud are discussed in the literature. The first form of employment fraud is that perpetrated against job seekers, where ‘a person with fraudulent intentions posts a fake job advertisement on an online platform’ (Mahbub and Pardede 2018: 1). Recruitment fraud in this context occurs when perpetrated against an individual victim seeking employment (Beals et al. 2015).

The second form of employment fraud centres on employers as the victim and job seeker as the fraud perpetrator. In this context, a fraudulent candidate seeks to defraud a potential employer by lying or providing misleading information about their employment history, qualifications, or another aspect of themselves (Button and Gee 2013; Gee et al. 2019). We use the term ‘recruitment fraud’ to refer to the first form of employment fraud. An offender uses deception to promote a fake job opportunity to a potential job seeker to gain a direct monetary reward or access to sensitive, personal details to gain a financial advantage indirectly. Several studies use the more specific term ‘online recruitment fraud’ (Lal et al. 2019; Mahbub and Pardede 2018; Mehboob and Malik 2021; Vidros et al. 2017). However, it should be noted that while such nomenclature recognises the predominantly online nature of this offence, differentiating the mode of attack may not be relevant or useful (Cross 2019a) as recruitment fraud occurs in both online and offline environments. Further, recruitment fraud can be targeted (such as jobs listing or untargeted [akin to spam]) (McCoy et al. 2016).

Offenders use several approaches to perpetrate recruitment fraud in this context. The first seeks to harvest personal information from potential employees. A fake job advertisement is posted, which attracts unsuspecting individuals to apply and upload sensitive information that offenders may compile into databases and on-sell to various legitimate and illegitimate groups (Vidros et al. 2016). Another approach uses the same ruse to obtain sensitive and personal information of potential employees. However, in this instance, the offenders themselves seek to use this to perpetrate identity crime on the unsuspecting victim. Documents sought after by offenders include social security numbers, identity cards, passports and bank account information. In this way, offenders can take on the victim’s identity or use their bank accounts to launder funds (Vidros et al. 2016, 2017).

A third approach occurs when offenders create fake advertisements and require upfront payments from potential candidates to cover services/fees related to their potential employment or pay for materials required for the position (Beals et al. 2015). Examples of this may include expenses associated with visas, training, travel or the purchase of starter kits (Mahbub and Pardede 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. A victim who complies with this will eventually be left with the costs associated with the full cheque amount and any amount withdrawn once the cheque is identified as counterfeit (Beals et al. 2015).

In all cases, victims lose personal details or money without receiving the promised employment outcome. In some cases, victims may realise what has occurred straight away, but in many circumstances, they may not realise what has occurred and believe they were not the preferred candidate. In reality, they were defrauded or likely subjected to identity crime. No specific studies have examined the effects of recruitment fraud on individuals. However, it is foreseeable that victims of these offences suffer the same gambit of financial and non-financial harms experienced by other fraud victims (Button et al. 2009; Button and Cross 2017; Cross 2019b), including self-blame and shame.

### Detection of Recruitment Fraud

It can be difficult to determine if a job advertisement is genuine or fake as there are often few observable differences. The structured format of job advertisements seeks to capture the attention of potential applicants (and victims) very quickly. However, it has been suggested that illegitimate opportunities can be identified as offering a disproportionately lucrative financial reward for flexible work requiring limited or no qualifications or experience (Mahbub and Perdede 2018; Youngblood 2015).

Given this difficulty, there is an emerging body of research that attempts to differentiate and identify fake job advertisements by drawing parallels to other areas of cybercrime, including phishing, spam, cyberbullying, opinion fraud, Wikipedia vandalism, fake news detection and trolling (Dutta and Bandyopadhyay 2020; Mahbub and Perdede 2018; Mehboob and Malik 2021; Vidros et al. 2017).

Much of the research in the area of online recruitment fraud has used a publicly available global dataset, the Employment Scam Aegean Dataset (EMSCAD) (see Alghamdi and Alharby 2019; Anita et al. 2021; Goya et al., 2021; Habiba et al., 2021; Keerthana et al, 2021; Mahbub and Pardede 2018; Mehboob and Malik 2021; Nindyati and Nugraha 2019; Ranparia et al., 2020; Shree et al., 2021; Vo et al. 2021). The EMSCAD data provided by the University of the Aegean comprises over 17,000 known genuine and around 800 fraudulent job advertisements published from 2012 to 2014. Researchers have created algorithmic models using this data that are purported to distinguish a fraudulent job advert from a legitimate one with a high percentage of accuracy. Such approaches rely on identifying characteristics and attributes that are more likely to be part of a fraudulent job advertisement than an authentic one. Variables used across these studies include those related to both content and metadata. Of particular interest to the exploration of recruitment fraud in the context of COVID-19 relates to the finding that fake advertisements offer individuals the ability to work from home at two times the rate of corresponding 'real' postings (Vidros et al. 2017).

Most fraudulent job ads within this dataset offered overpaid work-from-home positions (Vidros et al. 2016). Researchers have typically applied binary variables to the categories 'work from home' or 'telecommuting' (Mahbub and Perdede 2018) to determine if an advertisement is legitimate. These criteria are potentially problematic in ascertaining the presence or prevalence of recruitment fraud. The dataset on which many of these studies were based uses job advertisements collected between 2012 and 2014. Since then, there have been significant changes in practices associated with working from or near home due to technological advances and the necessity for social distancing created by the COVID-19 pandemic (Mikus et al. 2022).

### Prevalence of Recruitment Fraud and Victim Profile

There is a limited understanding or acknowledgement of the extent of recruitment fraud globally. Although much of the actual data has been collected by recruitment and job listing companies or government agencies through victim self-reports, it points to the issue as a significant problem that warrants further attention.

A 2015 survey by FlexJobs found 60 fraudulent job postings for every legitimate job. However, fewer than half of the applicants stated they were aware of the possibility of employment scams of this nature. Only seven per cent claimed to have been the victim of recruitment fraud at least once before (Vidros et al. 2016). No comparable peer-reviewed academic studies have been conducted to support or refute such claims.

Governments also collect statistics through a process of victim self-report. For example, victims in Canada and the United States of America can report recruitment fraud (under the label of employment scams) to the Better Business Bureau's *BBB Scam Tracker*. Between December 2019 and May 2020, over 13,000 job listing scams were reported on this site (Stahl 2020). The

Australian Competition and Consumer Commission (ACCC) collects and reports on fraud victimisation annually in Australia. The *Targeting Scams* report provides an overview of fraud approaches and victimisation based on reports to their Scamwatch online portal to report fraud in Australia. The *Targeting Scams* report also captures data from other relevant law enforcement agencies and financial institutions. The ACCC has a designated category of employment fraud, defined as those which 'trick you into handing over your money by offering you a "guaranteed" way to make fast money or a high-paying job for little effort' (ACCC 2020). Figure 1 provides an overview of reported employment fraud between 2018 and 2021. It shows an increase in total reports for 2020 and upward trending for the first half of 2021.

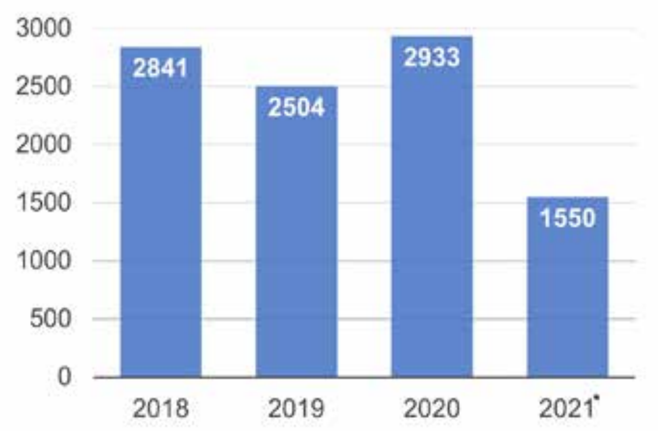

Figure 1. Number of reports of employment scams p.a, 2018–2021 (ACCC Scam Watch 2021)
* 2021 is a partial year reporting Jan–July only.

Despite some aggregate statistics, there is limited data available regarding the profile of the victims of recruitment fraud. Anecdotal evidence suggests that certain behaviours or characteristics might increase the exposure of job seekers to recruitment fraud. It is likely victims caught in fraudulent recruitment schemes are experiencing underemployment, such as a part-time worker seeking full-time employment (Policastro and Payne 2014) or seeking to improve their employment prospects. An example is the targeting of LinkedIn users for online recruitment fraud purposes. LinkedIn users typically utilise the site for professional advancement and professional self-presentation purposes, which can make them susceptible to exploitation (Alotaibi 2020). LinkedIn members may receive fake job offers via the platform, which lure them into sharing banking and other personal information (Franceschi-Bicchierai 2021). Recent articles in *Forbes* also highlight how using LinkedIn features such as the "#open to work' profile graphic can increase contacts from offenders and less reputable recruitment companies (Hellmann 2020). Indeed, it could be posited that because individuals are promoting themselves to the LinkedIn community as open to offers, they may be less suspicious of unsolicited contacts and could be exposed to phishing and other fraudulent activities.

## Conclusion

In recent years, fraud victimisation has continued to rise (ACCC 2021). The additional vulnerabilities emerging from the current global pandemic, and the potential for the effective targeting of fraud approaches, poses a significant threat against the wellbeing of individuals. This is particularly relevant in the case of recruitment fraud, given the rise in unemployment and underemployment combined with pre-existing employment precarity. COVID-19 has significantly altered the labour landscape, with organisations embracing remote and virtual working to unprecedented levels. Research conducted before the pandemic focused heavily on the offer of working from home (or telecommuting) as a red flag for fake job advertisements. While this may no longer be such an important predictor for fake job advertisements, the significant shift in working patterns and locations has the potential to encourage offenders to target the increasingly large pool of job seekers who will be attracted to this option. With an increased number of individuals subjected to working from home orders or experiencing isolation or lockdowns continually, offenders have also transitioned seamlessly to the online realm.

There are implications across many fronts. The current prevention messaging that focuses heavily on work-from-home scenarios as fraudulent is called into question. It further poses challenges to those who fall victim to these schemes and their ability to gain any form of justice through law enforcement responses. Further, there is a general inability to recover lost funds or restore their identities in the aftermath of identity theft or fraud, particularly where the fraudulent activity has occurred across jurisdictional boundaries.

Research on recruitment fraud is required on several fronts: first, research that quantifies the prevalence of recruitment fraud both in terms of fraudulent advertisements and victims falling prey to such deception is required. Second, research that compares contemporary fraudulent and fake advertisements to identify how offender approaches may be distinguished from legitimate job opportunities in the COVID-19 era is required. Third, because assumptions cannot be made about the victims of various forms of cyber fraud (Button and Cross 2017), research is required to understand the characteristics of those most susceptible to recruitment fraud so that targeted awareness materials can be developed. Finally, research is required to explore the important monitoring and detection role of job placement and posting sites to minimise the posting of fraudulent advertisements and safeguard their integrity.

## References

ACCC 2020, [Australian Competition and Consumer Commission] Targeting Scams 2019: *A Review of Scam Activity Since 2009*, https://www.accc.gov.au/

publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009 (Accessed 04/01/2022).

ACCC [Australian Competition and Consumer Commission] 2021 'Jobs and employment scams', *Scam Watch*, https://www.scamwatch.gov.au/types-of-scams/jobs-employment/jobs-employment-scams (accessed 04/01/2022).

Alghamdi, B. and Alharby, F. 2019 'An intelligent model for online recruitment fraud detection', *Journal of Information Security*, 10, 3: 155–176.

Alotaibi M. 2020 'Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: an empirical test', in N. Clarke and S. Furnell (eds) *Human Aspects of Information Security and Assurance*: HASIA 2021, Springer, 85–96.

Anita, C. Nagarajan, P. Sairam, G. Ganesh, P. and Deepakkumar, G. 2021 'Fake job detection and analysis using machine learning and deep learning algorithms', *Revista Geintec-Gestão Inovação e Tecnologias,* 11, 2: 642–650.

Baum, M. and Kabst, R. 2014 'The effectiveness of recruitment advertisements and recruitment websites: indirect and interactive effects on applicant attraction', *Human Resource Management*, 53, 3: 353–378.

Beals, M. DeLeima, M. and Deevy, M. 2015 *Framework for a Taxonomy of Fraud, Financial Fraud Research Centre*, Stanford Center on Longevity.

BBB [Better Business Bureau] 2021 *BBB Scam Tracker*, https://www.bbb.org/scamtracker (accessed 04/01/2022).

Blustein, D. and Guarino, P. 2020 'Work and unemployment in the time of COVID-19: the existential experience of loss and fear', *Journal of Humanistic Psychology*, 60, 5: 702–709.

Buil-Gil, D. Miró-Llinares, F. Moneva, A. Kemp, S. and Díaz-Castaňo, N. 2021a 'Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK', *European Societies*, 23, 1: 547–559.

Buil-Gil, D. Zeng, Y. and Kemp, S. 2021b 'Offline crime bounces back to pre-COVID levels, cyber stays high: interrupted time-series analysis in Northern Ireland', *Crime Science*, 10, 23: 1–16.

Button, M. and Cross, C. 2017 *Cyber Frauds, Scams and their Victims*, Routledge, London.

Button, M. and Gee, J. 2013 *Countering Fraud for Competitive Advantage: The Professional Approach to Reducing the Last Great Hidden Cost*, Wiley, London.

Button, M. Lewis, C. and Tapley, J. 2009 *A Better Deal for Victims: Research into Victims' Needs and Experiences*, National Fraud Authority, London.

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

Cross, C. 2019a 'Is online fraud just fraud? Examining the efficacy of the digital divide', *Journal of Criminological Research, Policy and Practice*, 5, 2: 120–131.

Cross, C. 2019b 'Online fraud', in Oxford Research *Encyclopedia of Criminology and Criminal Justice*, Oxford University Press.

Dutta, S. and Bandyopadhyay, S. 2020 'Fake job recruitment detection using machine learning approach', International *Journal of Engineering Trends and Technolog*y, 68, 4: 48–53.

Esoimeme, 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.

Fletcher, N. 2007 'Challenges for regulating financial fraud in cyberspace', *Journal of Financial Crime*, 14, 2: 190–207.

Franceschi-Bicchierai, L. 2021 'Scammers are sending fake job offers on LinkedIn', *Vice*, 20 January, https://www.vice.com/en/article/3an74y/scammers-are-sending-fake-job-offers-on-linkedin (accessed 22/12/2021)

Gee, J. Button, M. Wang, V. Blackbourn, D. and Shepherd, D. 2019 *The Real Cost of Recruitment Fraud,* Crowe and University of Portsmith, UK.

Goyal, N. Sachdeva, N. and Kumaraguru, P. 2021 'Spy the lie: fraudulent jobs detection in recruitment domain using knowledge graphs', *International Conference on Knowledge Science, Engineering and Managemen*t, Springer, 612–623.

Habiba, S. Islam, M. and Tasnim, F. 2021 'A comparative study on fake job post prediction using different data mining techniques', 2nd International Conference on Robotics, Electrical and Signal Processing Techniques, IEEE, 543–546.

Hellmann, R. 2020 'Job seekers: be careful using LinkedIn's new "Open To Work" feature', *Forbes*, 20 July, https://www.forbes.com/sites/roberthellmann/2020/07/20/job-seekers-be-careful-using-linkedins-new-open-to-work-feature/?sh=29066efd6138 (accessed 22/12/2021).

Keerthana, B. Reddy, A. and Tiwari, A. 2021 'Accurate prediction of fake job offers using machine learning', in D. Bhattacharyya and N. Thirupathi Rao (eds) *Machine Intelligence and Soft Computing,* Springer, 101–112.

Kemp, S. Buil-Gil, D. Moneva, A. Miró-Llinares and Díaz-Castaňo, N. 2021 'Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during COVID-19', *Journal of Contemporary Criminal Justice*, https://journals.sagepub.com/doi/full/10.1177/10439862211027986 (accessed 22/12/2021).

Kim, S. Wang, Y. and Boon, C. 2021 'Sixty years of research on technology and human resource management: looking back and looking forward', *Human Resource Management,* 60, 1: 229–247.

Lal, S. Jiaswal, R. Sardana, N. Verma, A. Kaur, A. and Mourya, R. 2019 'ORF detector: ensemble learning based online recruitment fraud detection', *12th International Conference on Contemporary Computing*, IEEE, 1–5.

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

McCoy, D. Park, Y. Shi, E. and Jakobsson, M. 2016 'Identifying scams and trends', in M. Jakobsson (ed) *Understanding Social Engineering Based Scams*, Springer, 7–19.

Mehboob, A. and Malik, M. 2021 'Smart fraud detection framework for job recruitments', *Arabian Journal for Science & Engineering*, 46, 4: 3067–3078.

Mikus, J. Rieger, J. and Grant-Smith, D. 2022 'Eudaemonic design for wellbeing at work wherever that may be', in M. Montoya-Reys, I. Medoza-Muñoz, G. Jacobo-Galicia, S. Cruz Sotelo and C. Novarro Gonzalez (eds) *Ergonomics and Business Policies for the Promotion of Well-Being in the Workplace*, igiGlobal.

Mukhlis, M. 2021 'Trafficking of women in Entikong Sub-District Sanggau Regency, Indonesia', *Jurnal Perspektif Pembiayaan dan Pembangunan Daerah*, 9, 2: 187–198.

Niharika Reddy, M. Mamatha, T. and Balaram, A. 2019 'Analysis of e-recruitment systems and detecting e-recruitment fraud', in A. Kumar and S. Mozar (eds) I*nternational Conference on Communications and Cyber Physical Engineering*, Lecture Notes in Electrical Engineering, 500, Springer.

Nindyati, O. and Nugraha, I. 2019 'Detecting scam in online job vacancy using behavioral features extraction', *International Conference on ICT for Smart Society*, 7: 1–4.

Nivette, A. Zahnow, R. Aguilar, R. Ahven, A. et al. (25 other authors). 2021 'A global analysis of the impact of COVID-19 stay-at-home restrictions on crime', *Natural Human Behavior,* 5: 868–877.

Payne, B. 2020 'Criminals work from home during pandemics too: a public health approach to respond to fraud and crimes against those 50 and above', *American Journal of Criminal Justice*, 45: 563–577.

Petre, A. Osoian, C. and Zaharie, M. 2016 'Applicants' perceptions on online recruitment', *Managerial Challenges of the Contemporary Society*, 9, 1: 63–67.

Policastro, C. and Payne, B. 2014 'Can you hear me now? Telemarketing fraud victimisation and lifestyles', *Southern Criminal Justice Association*, 40, 3: 620–638.

Ranparia, D. Kumari, S. and Sahani, A. 2020 'Fake job prediction using sequential network', *15th International Conference on Industrial and Information Systems*, IEEE, 339–343.

Shree, R. Nirmala, D. Sweatha, S. and Sneha, S. 2021 'Ensemble modeling on job scam detection', *Journal of Physics: Conference Series*, 1916, 1, https://jglobal.jst.go.jp/en/detail?JGLOBAL_ID=202102236119298249 (accessed 22/12/2021).

Stahl, A. 2020 'Job hunting scams amid COVID-19 pandemic', Forbes, 11 May, https://www.forbes.com/sites/ashleystahl/2020/05/11/job-hunting-scams-amid-covid-19-pandemic/?sh=1e9751a73c57 (accessed 22/12/2021).

Vidros, S. Kolias, C. and Kambourakis, G. 2016 'Online recruitment services: another playground for fraudsters', *Computer Fraud Security,* 3: 8–13.

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

Vo, M. Vo, A. Nguyen, T. Sharma, R. and Le, T. 2021 'Dealing with the class imbalance problem in the detection of fake job descriptions', *Computers, Materials and Continua*, 68, 1: 521–535.

Volodko, A. Cocknain, E. and 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.

Yar, M. and Steinmetz, K. 2019 *Cybercrime and Society* (3rd ed), Sage, London.

Youngblood, J. 2015 *A Comprehensive Look at Fraud Identification and Prevention*, CRC Press, Boca Raton, London, New York.

**Authors**

Dr Cassandra Cross is the Associate Dean (Learning and Teaching), Faculty of Creative Industries, Education and Social Justice, at Queensland University of Technology. She also holds a position as Associate Professor in the School of Justice, Queensland University of Technology. Her research focuses primarily on the policing, prevention, and victim support of fraud victims globally. She is co-author (with Mark Button) of the book *Cyber Frauds, Scams and Their Victims* published by Routledge in 2017.

Deanna Grant-Smith is an Associate Professor in the Faculty of Business and Law (QUT) and Deputy Director of the QUT Centre for Decent Work and Industry. Her research explores exploitative work practices including unpaid internships and multi-level marketing.

## Porter

It was a workplace where you'd likely clock out
but even on graveyard shifts as he wheeled
the last to go he'd listen to the hospital
rocking all night on the wave-hills,
steaming through dark its delivered freight,
the new in its relay race with the old,
late for its date with the end of the world.

He'd be first on deck, combing the quay
for the morning's early homecoming ships
where the old men and children sailed from each other
and a nurse from short ages past
who thought he was old as the century
said how it would be the end of the world
if today's first-born were the last.

Then the century grew young again
and, weary of his company
and the old women with their grandchildren,
went off without him, left him stuttering
seaward through a braille of bedrail,
a triangle of pain grimacing skin
down the slant of nose to the curl of lips,

tight on a lobstered-cold-blue skull.
He heaves at air now from shrunken shells
of lungs, wave-sick, riddled with light.
Helpless we come to earth, helpless we leave her,
he thinks, the old fools babes again,
and if these last-born lived for ever
that too would be the end of the world.

He's wheeled through it daily now, this portal
where the future's ships are crossing
whose passengers are always getting young
or babes that, bald and bare, become
again as old ones, born for burial.
They catch his breath, each gasp at landfall.
Not sea or shore, they see-saw, poised, rocking.

**Derek Wright**