LAWS6091 Special Interest Project

Olivia Shedden c3324507

Part 1: Research Paper

Introduction

Since its release in 2022, millions of Netflix users have tuned into the British true crime documentary *The Tinder Swindler* to learn the story of the Israeli fraudster Simon Leviev, who swindled his online girlfriends out of an estimated $10 million. The film shines a global light on romance scams, although perhaps the way in which it does so suggests to audiences that the scams are rare and fanciful. Contrary to any such misconception, romance scams have become an overwhelming reality for many individuals, especially in Australia. Underlying this subspecies of fraud is the complex psychology of scammers and the victims they choose to target, as well as a growing body of legal and regulatory postulations regarding the culpability of scammers and other third parties involved in the scams.

The purpose of this paper is to discuss how and why romance scams occur and explore developing legal and regulatory response, prevention and intervention actions against romance scams in Australia. The paper opens with a comprehensive summary of the context in which romance scams occur. This includes defining the scams, highlighting the increasing success of the scams with reference to statistics and social factors, outlining the scammers' motivations and the seven stages of the scams, and finally, profiling the vulnerabilities of victims and the impacts of victimhood. With that conceptual background in mind, the paper progresses to consider how criminal law and consumer law responses may apply to romance scams and highlights the various practical challenges victims face in pursuing legal action against scammers. In light of these challenges, the paper explores the current regulatory focus on developing prevention and intervention strategies, those being anti-scam campaigns to raise awareness and educate consumers, and improved regulations and funding to compel banks, dating apps and the police to intercept romance scams prior to completion. Finally, the paper contemplates how the recent establishment of the National Anti-Scam Centre presents a fresh opportunity to develop the aforementioned legal and regulatory response, prevention and intervention actions.

1 Context

1.1 Overview

1.1.1 Defining romance scams

The Australian Competition and Consumer Commission ("ACCC") defines dating and romance scams as follows:

> Scammers take advantage of people looking for love by pretending to be prospective partners, often via dating websites, apps or social media. They play on emotional triggers to get victims to provide money, gifts or personal details. Dating and romance scams can continue for years and they are increasingly introducing investment scams. They cause devastating emotional and financial damage.[1]

Dr Cassandra Cross, who has completed a Senior Research Fellowship with the Cybersecurity Cooperative Research Centre on the topic of romance fraud and is an Associate Dean and Associate Professor at the Queensland University of Technology, highlights that the key element is deception by way of a crafted relationship, which victims perceive as genuine and scammers exploit as a means to obtain financial gain.[2]

There are some suggestions that romance scams may date back to biblical times,[3] and in 21st century Western society, romance scams emerged in around 2008 via newspapers and mail advertisements.[4] However, in the past decade, romance scammers have found their stride online. In 2022, Dr Gregor Urbas, an Adjunct Associate Professor and Barrister at Australian National University, described romance scams as "perhaps the most startling cases… [the] fastest growing and lucrative species of online victimisation",[5] and noted deterrence is extremely difficult.[6]

1.1.2 The recent success of romance scams

Urbas' commentary is supported by the ACCC's data. Since 2010, romance scams have been in the top three categories of financial loss reported to the ACCC.[7] In 2010, 1149 reports to the ACCC via Scamwatch

---

[1] Australian Competition and Consumer Commission, *Targeting Scams Appendices: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 29.

[2] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 1.

[3] Yaniv Hanoch and Stacey Wood, 'Scams and Cryptocurrency Can Go Hand in Hand - Here's How They Work and What to Watch Out For' *The Conversation* (Online Article, 21 June 2022) https://theconversation.com/scams-and-cryptocurrency-can-go-hand-in-hand-heres-how-they-work-and-what-to-watch-out-for-182033.

[4] Monica Whitty and Tom Buchanan, 'The Online Romance Scam: A Serious Cybercrime' (2012) 15(3) *Cyberpsychology, Behavior and Social Networking* 181, 181.

[5] Sharon Givoni, 'Interview with Dr Gregor Urbas, Author of Cybercrime: Legislation, Cases and Commentary, 2nd edn' (2022) 24(9) *LexisNexis Internet Law Bulletin* 162, 166.

[6] Ibid.

[7] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2020* (Report, June 2021) 4; Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2021* (Report, July 2022) 5; Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 4.

accounted for $15.1 million in losses.[8] This has steadily increased to reach 3698 reports amounting to $40.5 million in losses in 2022.[9] Combining reports to Scamwatch with reports to ReportCyber, the Australian Financial Crimes Exchange ("AFCX"), the Australian Securities and Investments Commission ("ASIC") and IDCARE, there was a total of $210.2 million in losses reported in 2022.[10]

The recent success of romance scams can be attributed to at least two key factors. The evolution and increased use of technology has introduced a corresponding increased acceptance of online dating and social media platforms as a way to meet potential partners,[11] This increases scammers' access to millions of potential victims and thereby improves the commerciality of the scams.[12] Scammers' reach and profitability is further compounded by many individuals tending to believe what they read online and failing to appreciate the associated dangers of internet use, especially the lack of regulations surrounding internet access and content.[13]

Further, the number of potential victims has been exacerbated by increases in social isolation, loneliness and internet usage resulting from government restrictions relating to the Covid-19 pandemic.[14] During the pandemic, the community experienced ongoing anxiety and life strains, which likely wore down many people and made them more susceptible to fraud approaches that may not have worked prior to the pandemic.[15] For example, the pandemic gave scammers an acceptable reason to keep relationships online.[16] The relevant effects of the pandemic are best illustrated by considering Victoria, which was subject to intense government restrictions in the second wave of the pandemic in 2020, and simultaneously recorded the highest losses nationwide for the first time, totalling $49 million recorded losses to Scamwatch.[17]

1.2 Who are the scammers?

1.2.1 Catfishes and survivalists

There is very little information available about the identity of the scammers as scammers do not reveal their true identities.[18] Instead, they "catfish" victims, meaning they pretend to be other people by exploiting innocent people's online profiles or creating entirely fake identities.[19] In reality, most scammers are members of international crime syndicates,[20] sharing internet access, training each other and celebrating successful scams as a group.[21] Unsurprisingly, their principal motivation is financial gain.[22]

---

[8] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2010* (Report, 2021) 6.

[9] Australian Competition and Consumer Commission, 'Have a Heart-to-Heart With Loved Ones to Help Stop Scams This Valentine's Day' (Media Release 8/23, 12 February 2023).

[10] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 10.

[11] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 1.

[12] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 105.

[13] Michael Deacon, 'Bytes: There's Nothing Romantic About Online Fraud' (2010) 13(2) *LexisNexis Internet Law Bulletin* 40, 41.

[14] David Buil-Gil and Yongyu Zeng, 'Meeting You was a Fake: Investigating the Increase in Romance Fraud During COVID-19' (2022) 29(2) *Journal of Financial Crime* 460, 467.

[15] Cassandra Cross, 'Australians Lost $2b to Fraud in 2021. This Figure Should Sound Alarm Bells For the Future' *The Conversation* (Online Article, 6 July 2022) https://theconversation.com/australians-lost-2b-to-fraud-in-2021-this-figure-should-sound-alarm-bells-for-the-future-186459.

[16] Caitlin Fitsimmons, 'Lonely Australians Lose $200m to Romance Scams Amid Pandemic' *The Sydney Morning Herald* (online at 13 February 2022) https://www.smh.com.au/national/lonely-australians-lose-200m-to-romance-scams-amid-pandemic-20220208-p59up8.html.

[17] 'Scammers Capitalise on Pandemic as Australians Lose Record $851 Million to Scams' *Australian Competition and Consumer Commission Scamwatch* (News and Alerts, 7 June 2021) https://www.scamwatch.gov.au/news-alerts/scammers-capitalise-on-pandemic-as-australians-lose-record-851-million-to-scams.

[18] Griffiths News, 'Romance Scams - Anyone Can Fall Victim' *Griffith University* (Blog Post, 7 February 2018) https://news.griffith.edu.au/2018/02/07/romance-scams-anyone-can-fall-victim/.

[19] 'Catfishing' *eSafety Commissioner* (Web Page, No Date) https://www.esafety.gov.au/young-people/catfishing#:~:text=Something%20has%20happened-,What%20is%20catfishing%3F,they%20appear%20as%20someone%20else.

[20] Australian Federal Police, 'Love Actually Isn't All Around' (Media Release, 14 December 2022).

[21] Aunshul Rege, 'What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud' (2009) 3(3) *International Journal of Cyber Criminology* 494, 500.

[22] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 105.

Scammers' unscrupulous behaviour can be explained as a means to ensure survival.[23] Romance scammers are typically located in South and West African countries,[24] which are led by governments regarded as corrupt by international standards.[25] Executive corruption conveys to citizens that deceit is acceptable, which in conjunction with poverty, contributes to a heightened motivation to deceive victims for financial gain.[26]

1.2.2 Victims

However, not all scammers are willing participants. Many scammers operating in the syndicates are recruited as victims of the scams or via human trafficking, and then locked in basements and instructed on how to scam.[27] An Australian volunteer working at the Global Anti-Scam Organisation described:

> Some of these people are not willingly in these roles. Their working conditions are really bad, like sweatshop conditions. The only way out of it is if you scam enough people. The only way that they can escape is to rip people off.[28]

1.3 How do the scammers operate?

Fortunately, the ACCC, the Australian Federal Police ("AFP") and researchers have substantial knowledge as to how scammers execute romance scams. Although scammers often tailor the scams to exploit each victim's circumstances and continually innovate their methods to avoid detection,[29] the common aspects of romance scams can be explained with reference to Whitty's persuasive techniques model:[30]

Stage 1	Motivated to find the ideal partner
Stage 2	Presented with the fake profile
Stage 3	Grooming process
Stage 4	The sting
Stage 5	Continuation of the scam
Stage 6	Sexual abuse
Stage 7	Re-victimisation

1.3.1 Stage 1: Motivated to find the ideal partner

Whitty suggests that romance scams start with potential victims hoping to meet new partners and being open to that occurring via online dating.[31] However, in 2019 then-Deputy Chair of the ACCC, Delia Rickard, identified the start of a new trend whereby scammers contact victims on non-dating social media apps or games, including Google Hangouts, Words with Friends and Scrabble.[32] It follows that scammers will target victims on any

---

[23] Ken Rotenberg, 'Inside the Mind of the Online Scammer' *The Conversation* (Online Article, 20 December 2019) https://theconversation.com/inside-the-mind-of-the-online-scammer-127471.

[24] Griffiths News, 'Romance Scams - Anyone Can Fall Victim' *Griffith University* (Blog Post, 7 February 2018) https://news.griffith.edu.au/2018/02/07/romance-scams-anyone-can-fall-victim/.

[25] Ken Rotenberg, 'Inside the Mind of the Online Scammer' *The Conversation* (Online Article, 20 December 2019) https://theconversation.com/inside-the-mind-of-the-online-scammer-127471.

[26] Ibid.

[27] James Purtill, 'Anthony Message with 'Michelle' Every Day For Months. He was Drained of His Savings in an Elaborate 'Pig Butchering' Scam' *ABC News* (online at 6 November 2022) https://www.abc.net.au/news/2022-11-07/pig-butchering-crypto-romance-investment-scams/101606644.

[28] Ibid.

[29] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2.

[30] Monica Whitty, 'The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam' (2013) 53(4) *British Journal of Criminology* 665, 676 – 81.

[31] Ibid, 676.

[32] 'Romance Scammers Move to New Apps, Costing Aussies More Than $28.6 Million' *Australian Competitions and Consumer Commission Scamwatch* (News and Alerts, 9 February 2020) https://www.scamwatch.gov.au/news-alerts/romance-scammers-move-to-new-apps-costing-aussies-more-than-286-million.

online platform, irrespective of whether the victim is overtly looking for a partner.[33]

1.3.2 Stage 2: Presented with the fake profile

Scammers create fake profiles which are designed to lure in victims.[34] They purchase hundreds of photos and videos of the same people from websites which have taken the content from social media profiles and created categories for personas such as "beautiful young women" or "handsome middle-aged men".[35] Scammers often select trusted occupations, such as army personnel, humanitarians, oil rig workers, or professional service providers including engineers, lawyers and doctors.[36] They garner sympathy from victims by claiming to be widowers from Australia or other western countries but travelling or working overseas.[37] Overall, scammers rely upon their personas' attractiveness, authority and relatability to increase the likelihood that victims will want to form relationships with them and will later comply with requests for money.[38]

1.3.3 Stage 3: Grooming process

Once scammers and victims connect online, the scams progress to the grooming stage, which is characterised by scammers building rapport and manipulating victims.[39] Scammers spend months building the romance of a lifetime,[40] including sharing early and intense professions of love ("love bombing"), telling personal stories about unsuccessful past relationships or traumatic events, sending expensive gifts and pretending to book flights to visit.[41] During this stage, scammers are also likely to suggest moving the relationships to more personal means of communication such as phone messaging or email, which is to ensure the initial platforms cannot delete their profiles and law enforcement cannot access the communication logs.[42] Ultimately, scammers use grooming to convince victims they are in a relationship and to gain confidence in their ability to successfully request money.[43] As Rickard summarised:

> Scammers usually have a good understanding of who this person is through looking at what they like and don't like. They are highly skilled at manipulating their victims' emotions. These people make a lot of effort to groom their victims. They'll be incredibly thoughtful and create a dream universe just for the two of you. Then they will eventually ask for money. They all lead to money.[44]

1.3.4 Stage 4: The sting

"The sting" is the critical stage where, sensing that trust has been gained and defences are down, scammers start asking victims for money or bank/credit card details.[45] Dr Jacqueline Drew, Associate Professor at Griffith University's School of Criminology and Criminal Justice, highlights that the big red flag is the time sensitivity

---

[33] Ibid.

[34] Cassandra Cross and Rebecca Layt, ''I Suspect That the Pictures Are Stolen' Romance Fraud, Identity Crime and Responding to Suspicions of Inauthentic Identities' (2021) 40(4) *Social Science Computer Review* 955, 956.

[35] James Purtill, 'Anthony Message with 'Michelle' Every Day For Months. He was Drained of His Savings in an Elaborate 'Pig Butchering' Scam' *ABC News* (online at 6 November 2022) https://www.abc.net.au/news/2022-11-07/pig-butchering-crypto-romance-investment-scams/101606644.

[36] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2; 'Romance Scams', *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

[37] Ibid.

[38] Jacqueline Drew and Cassandra Cross, 'Fraud and Its PREY: Conceptualising Social Engineering Tactics and Its Impact On Financial Literacy Outcomes' (2013) 18(3) *Journal of Financial Services Marketing* 188, 194; Cassandra Cross, '$2.5 Billion Lost Over a Decade: 'Nigerian Princes' Lose Their Sheen, But Scams Are On the Rise' *The Conversation* (Online Article, 6 July 2020) https://theconversation.com/2-5-billion-lost-over-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289.

[39] Helen Whittle et al, 'A Review of Online Grooming: Characteristics and Concerns' (2013) 18 *Aggression and Violent Behaviour* 62, 64 – 5.

[40] 'Romance Scams', A*ustralian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

[41] Australian Competition and Consumer Commission, 'Have a Heart-to-Heart With Loved Ones to Help Stop Scams This Valentine's Day' (Media Release 8/23, 12 February 2023).

[42] Ibid.

[43] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2.

[44] Helen Signy, 'Lonely Heart Scams: What Seemed a Genuine Romance Ultimately Left One Woman Devastated' *Australia Reader's Digest* (Blog Post) https://www.readersdigest.com.au/money/lonely-heart-scams.

[45] 'Romance Scams', *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

of the transfer of the money.[46] Scammers invent elaborate reasons why they need money, which always includes a sense of urgency as a social engineering technique to stop victims from thinking before making the payment,[47] and usually relates to the scenario they have created to further increase the likely success of the scam.[48] Drew identifies that the reasons often target the progression of the relationship:

> It's usually to establish the relationship that they ask for the first request of money which of course makes the person excited that their new boyfriend or girlfriend is about to visit them…Then we see a whole series of catastrophic events occur to the offender such as being caught up in customs or corrupt officials at the airport who require money, or they have an accident on the way to the airport.[49]

Otherwise, requests may relate to business operations, such as needing money to pay for an aspect of employment, medical needs, such as needing money to pay for injuries or illnesses suffered by them or their children, or criminal justice needs, such as having been arrested.[50] To ensure the transfers appear ordinary, scammers coach victims on what to write in payment descriptions and how to answer any questions.[51]

At this stage, it is worth noting two prevalent subspecies of romance scams which deviate from traditional requests for money: romance baiting and money laundering. Romance baiting, which essentially combines investment scams with romance scams and is reported as the latter,[52] involves scammers subtly persuading victims to transfer funds into their account under the guise of investing in a money-making scheme, which is usually cryptocurrency.[53] After grooming victims by casually talking about learning crypto trading from family members and investing large sums into their own portfolios,[54] scammers coach victims on investing small amounts to prove how easy it is,[55] and then create fake data on victims' accounts to reflect substantial profits.[56]

Scammers encourage victims to deposit more funds, and eventually manipulate the data to show losses.[57] When victims ask to withdraw the funds, scammers will cease contact or demand further payments for "release of funds" before disappearing.[58] Romance scammers exploit the increasing popularity and sophistication of

---

[46] Griffiths News, 'Romance Scams - Anyone Can Fall Victim', *Griffith University* (Blog Post, 7 February 2018) https://news.griffith.edu.au/2018/02/07/romance-scams-anyone-can-fall-victim/.

[47] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2; Cassandra Cross, '$2.5 Billion Lost Over a Decade: 'Nigerian Princes' Lose Their Sheen, But Scams Are On the Rise' *The Conversation* (Online Article, 6 July 2020) https://theconversation.com/2-5-billion-lost-over-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289.

[48] Ibid.

[49] Griffiths News, 'Romance Scams - Anyone Can Fall Victim', *Griffith University* (Blog Post, 7 February 2018) https://news.griffith.edu.au/2018/02/07/romance-scams-anyone-can-fall-victim/.

[50] Monica Whitty, 'The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam' (2013) 53(4) *British Journal of Criminology* 665, 679; 'Romance Scams', *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

[51] Jessica Yun, 'Sextortion and 'Very Expensive Heartbreak': Beware Valentine's Day Scams, says ACCC' *The Sydney Morning Herald* (online at 14 February 2023) https://www.smh.com.au/business/consumer-affairs/sextortion-and-very-expensive-heartbreak-beware-valentine-s-day-scams-says-accc-20230212-p5cjuk.html.

[52] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 13, 32; Cassandra Cross, 'Australians Lost More Than $3bn to Scammers in 2022. Here Are 5 Emerging Scams to Look Out For' *The Conversation* (Online Article, 21 April 2023) https://theconversation.com/australians-lost-more-than-3bn-to-scammers-in-2022-here-are-5-emerging-scams-to-look-out-for-204018.

[53] 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/; Cassandra Cross, 'Australians Lost More Than $3bn to Scammers in 2022. Here Are 5 Emerging Scams to Look Out For' *The Conversation* (Online Article, 21 April 2023) https://theconversation.com/australians-lost-more-than-3bn-to-scammers-in-2022-here-are-5-emerging-scams-to-look-out-for-204018.

[54] James Purtill, 'Anthony Message with 'Michelle' Every Day For Months. He was Drained of His Savings in an Elaborate 'Pig Butchering' Scam' *ABC News* (online at 6 November 2022) https://www.abc.net.au/news/2022-11-07/pig-butchering-crypto-romance-investment-scams/101606644.

[55] 'Romance Baiting Scams on the Rise' *Australian Competition and Consumer Commission Scamwatch* (News and Alerts, 12 February 2021) https://www.scamwatch.gov.au/news-alerts/romance-baiting-scams-on-the-rise.

[56] 'Scam Alert: ASIC Sees a Rise in Crypto Scams' Australian Securities and Investments Commission (News and Alerts) https://asic.gov.au/about-asic/news-centre/news-items/scam-alert-asic-sees-a-rise-in-crypto-scams/.

[57] Ibid.

[58] Ibid.

cryptocurrency trading to tap into unique benefits,[59] such as greater perceived legitimacy via fake wallets, affiliate websites and correspondence from customer representatives,[60] enhanced anonymity in transactions and less opportunity for third party intervention.[61]

Romance scams are also a vehicle for scammers to recruit mules for money laundering. Scammers may ask victims to send or forward funds or receive or purchase goods, and the transactions usually involve international friends, family and businesses.[62] In reality, scammers are trying to move proceeds from criminal activities, including drug sales, firearms trade and online scams,[63] and try to use victims' legitimate Australian bank accounts to avoid the transactions being detected or traced by anti-money laundering organisations such as the Australian Transaction Reports and Analysis Centre ("AUSTRAC").[64]

Victims may not be scammed out of money, but they may be prosecuted for dealing with proceeds of crime if they were knowingly involved. For example, in *R v Ogbeide*,[65] the defendant, who was involved in a criminal syndicate carrying out online romance scams and received proceeds into his bank account which he used to purchase Bitcoin, was prosecuted of 11 offences, including multiple knowingly or recklessly dealing with proceeds of crime.[66]

1.3.5 Stage 5: Continuation of the scam

Victims who comply with initial requests for finances are then subject to further requests escalating in amount and frequency.[67] Scammers utilise psychological abuse techniques such as isolating victims from their friends and family, fostering secrecy about the nature of the relationship and continually degrading victims.[68] By doing so, scammers remove opportunities for victims to be warned about scams and perpetrate traits of domestic violence and coercive control against the victims.[69] This enables the scammers to maintain their powers to continually persuade victims to provide financial assistance,[70] while the victims are stuck in cycles of trying to satisfy their addiction to toxic relationships.[71] This stage can be sustained for weeks, months or years.[72]

1.3.6 Stage 6: Sexual abuse

In some circumstances, scammers may employ "sextortion" tactics by using intimate images or recordings

---

[59] Yaniv Hanoch and Stacey Wood, 'Scams and Cryptocurrency Can Go Hand in Hand - Here's How They Work and What to Watch Out For' *The Conversation* (Online Article, 21 June 2022) https://theconversation.com/scams-and-cryptocurrency-can-go-hand-in-hand-heres-how-they-work-and-what-to-watch-out-for-182033.

[60] Ibid.

[61] James Purtill, 'Anthony Message with 'Michelle' Every Day For Months. He was Drained of His Savings in an Elaborate 'Pig Butchering' Scam' *ABC News* (online at 6 November 2022) https://www.abc.net.au/news/2022-11-07/pig-butchering-crypto-romance-investment-scams/101606644.

[62] Australian Federal Police, 'Love Actually Isn't All Around' (Media Release, 14 December 2022); 'Romance Scams', *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

[63] Australian Federal Police, 'Love Actually Isn't All Around' (Media Release, 14 December 2022);

[64] Tara Cassidy, 'Romance Scam Money Laundering on the Rise ACCC Warns Victims Can Face Jail Time' *ABC News* (online at 3 October 2020) https://www.abc.net.au/news/2020-10-03/accc-says-romance-scams-being-used-for-money-laundering/12726730.

[65] [2021] NSWDC 750.

[66] *Crimes Act 1900* (NSW) s 193B; *R v Ogbeide* [2021] NSWDC 750, [1]-[9] (M L Williams SC DCJ).

[67] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2.

[68] Cassandra Cross, '$2.5 Billion Lost Over a Decade: 'Nigerian Princes' Lose Their Sheen, But Scams Are On the Rise' *The Conversation* (Online Article, 6 July 2020) https://theconversation.com/2-5-billion-lost-over-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289.

[69] Danielle Maguire and Nicholas McElroy, 'Think Your Relative is Caught Up in a Romance Scam? Here's How to Talk to Them About Love Scams This Valentine's Day' *ABC News* (online at 14 February 2023) https://www.abc.net.au/news/2023-02-14/romance-scams-how-to-help-online-dating-valentines-day/101959558.

[70] Cassandra Cross, Molly Dragiewicz and Kelly Richards, 'Understanding Romance Fraud: Insights From Domestic Violence Research' (2018) 58 *British Journal of Criminology* 1303, 1318.

[71] Danielle Maguire and Nicholas McElroy, 'Think Your Relative is Caught Up in a Romance Scam? Here's How to Talk to Them About Love Scams This Valentine's Day' *ABC News* (online at 14 February 2023) https://www.abc.net.au/news/2023-02-14/romance-scams-how-to-help-online-dating-valentines-day/101959558.

[72] Cassandra Cross, Molly Dragiewicz and Kelly Richards, 'Understanding Romance Fraud: Insights From Domestic Violence Research' (2018) 58 *British Journal of Criminology* 1303, 1318.

obtained during the relationship as a tool to blackmail victims into sending more money.[73]

1.3.7 Stage 7: Re-victimisation

Once victims have been successfully scammed, they are more likely to be further targeted and victimised.[74] This can occur in two ways: first, by scammers trading lists of their victims and repeatedly targeting those who have previously sent money, or alternatively, by scammers posing as authorities aiming to help victims retrieve funds lost to the first schemes.[75]

1.4 Who are the victims?

Most Australians have their physiological needs and safety met, which leaves them looking to find human connection and love.[76] Considering most of the population also has internet access, this makes Australians desirable victims for romance scammers.[77] Romance scammers target all sectors of the community, however the common thread across all scams is one or more factors making victims vulnerable to romantic exploitation.[78]

1.4.1 Older persons

The ACCC's data identifies particular community groups who are most likely to be vulnerable online. In 2021, people over 55 years of age reported $25 million in losses to romance scams to the ACCC, which accounted for nearly half of all losses that year.[79] Scammers target older persons because they are more likely to have wealth and to be divorced or widowed.[80] Professor David Lacey of IDCARE highlights there is a relationship between victims' susceptibility to romance scams and significant events occurring in their life such as family deaths, relationship breakdown, job losses, health concerns.[81] Scammers look for online profiles mentioning these events or other sources of emotional vulnerability.[82]

1.4.2 Younger persons

In comparison, younger persons are less likely to have substantial assets and histories of significant long-term relationships,[83] however they are more susceptible to niches within traditional romance scams. For example, almost half of all losses to romance baiting scams come from victims under the age of 35,[84] who are predominantly first-time investors and therefore susceptible to fake investment advice.[85] This age group,

---

[73] Roberta Liggett O'Malley and Karen Holt, 'Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime' (2020) 37(1-2) *Journal of Interpersonal Violence* 258, 258; Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2.

[74] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 2.

[75] Ibid.

[76] 'The Lure of Romance Scams', *National Criminal Lawyers* (Blog Post, 19 June 2020) https://www.nationalcriminallawyers.com.au/the-lure-of-romance-scams/#:~:text=THE%20LAW,for%20up%20to%2010%20years.

[77] Marilyn Krawitz, 'Stop! In the Name of Fraud, Before You Break Your Bank Account: Actions to Take When Your Client is the Victim of Online Dating Fraud' (2013) 16(3) *Internet Law Bulletin* 75, 75 – 6.

[78] 'Culturally and Linguistically Diverse Community Loses $22 Million to Scams in 2020, Reports From Indigenous Australians Up 25 Per Cent' *Australia Competition and Consumer Commission Scamwatch* (News and Alerts, 10 June 2021) https://www.scamwatch.gov.au/news-alerts/culturally-and-linguistically-diverse-community-lose-22-million-to-scams-in-2020-reports-from-indigenous-australians-up-by-25-per-cent.

[79] 'Learn How to Spot a Romance Scammer This Valentine's Day' *Australia Competition and Consumer Commission Scamwatch* (News and Alerts, 14 February 2022) https://www.scamwatch.gov.au/news-alerts/learn-how-to-spot-a-romance-scammer-this-valentines-day.

[80] Nicola Field, 'Romance Scams: It's Not Love, Actually', *Money* (Blog Post, 19 April 2023) https://www.moneymag.com.au/how-to-spot-a-romance-scam.

[81] Jessica Lamb, 'Sinister COVID Trend Sees Online Love Scams Target Younger Victims' *ABC News* (online at 11 May 2021) https://www.abc.net.au/news/2021-05-11/covid-love-scams-target-younger-victims/100064644.

[82] Ibid.

[83] 'Policymakers Beginning to Address the Scrouge of Romance Scams', *LexisNexis* (Blog Post, 31 March 2022) https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/policymakers-beginning-to-address-the-scourge-of-romance-scams.

[84] Cassandra Cross, '$2.5 Billion Lost Over a Decade: 'Nigerian Princes' Lose Their Sheen, But Scams Are On the Rise' *The Conversation* (Online Article, 6 July 2020) https://theconversation.com/2-5-billion-lost-over-a-decade-nigerian-princes-lose-their-sheen-but-scams-are-on-the-rise-141289.

[85] James Purtill, 'Anthony Message with 'Michelle' Every Day For Months. He was Drained of His Savings in an Elaborate 'Pig Butchering' Scam' *ABC News* (online at 6 November 2022) https://www.abc.net.au/news/2022-11-07/pig-butchering-crypto-romance-investment-scams/101606644.

especially males, are also more likely to be scammed out of money by way of sextortion.[86]

1.4.3 Ethic, cultural or linguistic background

Unfortunately, scammers also try to target people who may be vulnerable due to their ethnic, cultural or linguistic background or disability.[87] In 2022, romance scams were the second most prevalent scam type across these sectors, with reported losses being $764,000.00 from Aboriginal and Torres Strait Islander victims,[88] $6.6m from culturally and linguistically diverse victims,[89] and $4.6 million from victims with disabilities.[90]

1.5 How do the victims suffer?

1.5.1 Finances, relationships and health

Romance scams are described as a unique "double hit" of victimisation.[91] Not only do victims suffer significant financial losses which can impact on their mortgage repayments and retirement plans,[92] they also grieve the loss of their relationships, which for some victims causes greater trauma and is more difficult to cope with and recover from than the monetary losses.[93] Victims may face deteriorating physical health and emotional wellbeing, depression, unemployment, homelessness and suicide.[94] Some victims also have to deal with the repercussions of scammers stealing their personal information to use for identity frauds.[95]

Increasingly, victims are unable to accept the reality of the scam and instead believe scammers' excuses and explanations as to why they need financial assistance.[96] In such cases, victims are highly likely to remain in the continuation of scams for extended periods,[97] and may be tempted to travel overseas to meet their partners, which presents risks of physical assault or death.[98] For example, in 2012, an elderly Western Australian woman named Jette Jacobs travelled to South Africa to meet her Nigerian online love interest, and was later found dead in suspicious circumstances including the theft of $120,000.00 of her money as well as her credit cards, jewellery and laptop.[99]

1.5.2 Stigmatisation

Victims are also subjected to high levels of stigmatisation associated with being involved in romance scams.[100] Although romance scammers have become highly sophisticated and extremely difficult to identify, there is a perception that victims must be unintelligent to be so "blinded by love",[101] and that victims are greedy, gullible

---

[86] Jessica Yun, 'Sextortion and 'Very Expensive Heartbreak': Beware Valentine's Day Scams, says ACCC' *The Sydney Morning Herald* (online at 14 February 2023) https://www.smh.com.au/business/consumer-affairs/sextortion-and-very-expensive-heartbreak-beware-valentine-s-day-scams-says-accc-20230212-p5cjuk.html.

[87] 'Culturally and Linguistically Diverse Community Loses $22 Million to Scams in 2020, Reports From Indigenous Australians Up 25 Per Cent' *Australia Competition and Consumer Commission Scamwatch* (News and Alerts, 10 June 2021) https://www.scamwatch.gov.au/news-alerts/culturally-and-linguistically-diverse-community-lose-22-million-to-scams-in-2020-reports-from-indigenous-australians-up-by-25-per-cent.

[88] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 22.

[89] Ibid 23.

[90] Ibid 24.

[91] Monica Whitty and Tom Buchanan, 'The Online Romance Scam: A Serious Cybercrime' (2012) 15(3) *Cyberpsychology, Behavior and Social Networking* 181, 181.

[92] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 106.

[93] Cassandra Cross, Kelly Richards and Russell Smith, *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support* (Grant CRG 29/13-14, August 2016) 24.

[94] Ibid 19 – 34.

[95] Marilyn Krawitz, 'Stop! In the Name of Fraud, Before You Break Your Bank Account: Actions to Take When Your Client is the Victim of Online Dating Fraud' (2013) 16(3) *Internet Law Bulletin* 75, 75.

[96] Australian Federal Police, 'When Love Hurts: A Warning to Lonely Hearts' (Media Release, 14 February 2023).

[97] Natalie Gately and James McCue, 'A Handsome Soldier With a 'Medical Bill': How Romance Scammers Make You Fall in Love With Them' *The Conversation* (Online Article, 28 November 2019) https://theconversation.com/a-handsome-soldier-with-a-medical-bill-how-romance-scammers-make-you-fall-in-love-with-them-127820.

[98] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd ed, 2015) 215.

[99] Sharon Givoni, 'Interview with Dr Gregor Urbas, Author of Cybercrime: Legislation, Cases and Commentary, 2nd edn' (2022) 24(9) *LexisNexis Internet Law Bulletin* 162, 166.

[100] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 3.

[101] Tara Cassidy, 'Romance Scam Money Laundering on the Rise ACCC Warns Victims Can Face Jail Time' *ABC News* (online at 3 October 2020) https://www.abc.net.au/news/2020-10-03/accc-says-romance-scams-being-used-for-money-laundering/12726730.

and somewhat deserving of the scams.[102] Victims are usually aware of the negative connotations and ridicule.[103] Their internalised feelings of shame, humiliation and violation acts as a barrier to them seeking support.[104] Victims avoid telling their friends and family about what has occurred due to fear of angry or upset responses and ending those relationships.[105]

When victims do tell their support networks, they may characterise the discussions with some humour to distance themselves from acknowledging their own vulnerabilities, however this coping mechanism reinforces and normalises victim blaming.[106] Victims are often met by a total lack of understanding, thus further compounding the psychological damage of the scams.[107] Similarly, only 13% of victims make reports to Scamwatch,[108] with the balance likely feeling too embarrassed to do so.[109] Victims who do report the scams can experience additional trauma within the reporting systems.[110] Victims also forgo medical assistance to improve their physical and psychological wellbeing, financial counselling to assist with their financial losses, and counselling to repair relationships with their friends and family, if disclosed.[111]

2 Responses

Romance scams fall within the ambit of both the Australian consumer law and criminal law systems.[112] While potential avenues to prosecute scammers have emerged within the criminal law system, the consumer law system appears to be focused on developing actions for victims to take against banks involved in the scams. Irrespective of the differences, both jurisdictions face similar challenges in achieving justice for victims of romance scams. Each of these matters are further explored below.

2.1 Criminal law

2.1.1 Legislative framework

In considering the criminalisation of romance scams, the appropriate starting point is the Council of Europe Convention on Cybercrime ("the Budapest Convention").[113] The Budapest Convention is the most comprehensive international agreement on cybercrime and serves as a guideline for countries developing legislation on cybercrime as well as a framework for international cooperation between parties.[114] Relevantly, Article 8 addresses computer-related fraud, stating:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

---

[102] Cassandra Cross, 'No Laughing Matter: Blaming the Victim of Online Fraud' (2015) 21(2) *International Review of Victimology* 187, 187.
[103] Ibid.
[104] Cassandra Cross, Kelly Richards and Russell Smith, *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support* (Grant CRG 29/13-14, August 2016) 71.
[105] Ibid.
[106] Cassandra Cross, 'No Laughing Matter: Blaming the Victim of Online Fraud' (2015) 21(2) *International Review of Victimology* 187, 187 – 8.
[107] Natalie Gately and James McCue, 'A Handsome Soldier With a 'Medical Bill': How Romance Scammers Make You Fall in Love With Them' *The Conversation* (Online Article, 28 November 2019) https://theconversation.com/a-handsome-soldier-with-a-medical-bill-how-romance-scammers-make-you-fall-in-love-with-them-127820.
[108] 'Learn How to Spot a Romance Scammer This Valentine's Day' *Australia Competition and Consumer Commission Scamwatch* (News and Alerts, 14 February 2022) https://www.scamwatch.gov.au/news-alerts/learn-how-to-spot-a-romance-scammer-this-valentines-day.
[109] 'Romance Scams', *Crime Stoppers* (Resources Page) https://crimestoppers.com.au/resource/romance-scams/.
[110] Cassandra Cross, Kelly Richards and Russell Smith, *Improving Responses to Online Fraud Victims: An Examination of Reporting and Support* (Grant CRG 29/13-14, August 2016) 6 – 7.
[111] Helen Signy, 'Lonely Heart Scams: What Seemed a Genuine Romance Ultimately Left One Woman Devastated' *Australia Reader's Digest* (Blog Post) https://www.readersdigest.com.au/money/lonely-heart-scams.
[112] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 110.
[113] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS 185 (entered into force 1 July 2004) ('*Budapest Convention*').
[114] Council of Europe Portal, 'The Budapest Convention (ETS No. 185) and Its Protocols' *Cybercrime* (Web Page, No Date) https://www.coe.int/en/web/cybercrime/the-budapest-convention.

a. any input, alteration, deletion or suppression of computer data,
b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[115]

Urbas summarises Article 8 to comprise of four essential elements: computer-related acts; resulting in inauthentic (altered or interfered with) data; being presented as genuine; and to obtain economic benefit.[116] Although there are no specific criminal offences in any Australian criminal jurisdictions which specifically address online frauds, romance-related or otherwise, in *United States of America v Griffiths*,[117] Jacobson J affirmed the application of general fraud criminal offences to online fraud cases, explaining:

> First, internet fraud, though relatively new, involves nothing more than an application of the legal principles applicable to communication by post and telegraph…True it is that the Internet has a wider reach and wider field of applications but the problem of widely disseminated communication is…much older than the Internet and the World Wide Web…[T]he law has had to grapple with cases of this kind ever since newspapers and magazines, and later radio and television, came to be made available to large numbers of people over wide geographic areas. To this may be added telephones, mobile phones and fax machines.[118]

In light of His Honour's commentary, Urbas explains that the elements of online fraud are encapsulated by the general fraud criminal offences, which are summarised below:[119]

Jurisdiction	**Provision**	**Physical elements**	**Mental elements**	**Maximum penalty**
Australian Capital Territory	*Criminal Code 2002* (ACT) s 326 (Obtaining property by deception)	By a deception, obtaining from another person property belonging to someone else	Dishonestly, with intention of permanently depriving the other person	Imprisonment for 10 years or 1000 penalty units or both
	Criminal Code 2002 (ACT) s 332 (Obtaining financial advantage by deception)	By deception, obtaining financial advantage from someone else	Dishonestly	Imprisonment for 10 years or 1000 penalty units or both
New South Wales	*Crimes Act 1900* (NSW) s 192E (Fraud)	By deception, obtaining property belonging to another or financial advantage	Dishonestly	Imprisonment for 10 years
Northern Territory	*Criminal Code Act* (NT) s 227 (Criminal deception)	By deception, obtaining property belonging to another or financial advantage	Not specified	As for stealing property of the same value; or imprisonment for seven years where credit is obtained

[115] *Budapest Convention* art 6.
[116] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 111.
[117] [2004] FCA 879.
[118] *United States of America v Griffiths* [2004] FCA 879, [117] – [118] (Jacobson J).
[119] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 113 – 5.

Queensland	*Criminal Code Act 1899* (QLD) s 408C (Fraud)	Obtaining property or a benefit, etc	Dishonestly	Imprisonment for five years; 12 years if in position of authority or where value is over $30,000.00
South Australia	*Criminal Law Consolidation Act 1935* (SA) s 139 (Deception)	Deceiving another to obtain a gain or cause a loss	Dishonestly	Imprisonment for 10 years; 15 years if aggravated
Tasmania	*Criminal Code Act 1924* (Tas) s 250 (Obtaining goods by false pretences)	By any false pretence, obtaining goods	With intent to defraud	A general maximum penalty of 21 years applies to Criminal Code offences
	Criminal Code Act 1924 (Tas) s 253A (Fraud)	By deceit or any fraudulent means, obtaining property, etc	With intent to defraud	A general maximum penalty of 21 years applies to Criminal Code offences
	Criminal Code Act 1924 (Tas) s 257B (Computer-related fraud)	Destroying, damaging, erasing, altering or otherwise manipulating computer data, etc	With intent to defraud	A general maximum penalty of 21 years applies to Criminal Code offences
Victoria	*Crimes Act 1958* (Vic) s 81 (Obtaining property by deception)	By deception, obtaining property belonging to another	Dishonestly	Imprisonment for 10 years
	Crimes Act 1958 (Vic) s 82 (Obtaining financial advantage by deception)	By deception, obtaining financial advantage	Dishonestly	Imprisonment for 10 years
Western Australia	*Criminal Code Act Compilation Act 1913* (WA) s 409 (Fraud)	By deceit or any fraudulent means, obtaining property, etc	With intent to defraud	Imprisonment for seven years; 10 years if victim is over 60 years old

2.1.2 Case examples

Urbas' observations are demonstrated by some Australian cases on point. For example, in the case of *R v Lancaster*,[120] an Australian woman pleaded guilty to 10 offences of obtaining property by deception.[121] The defendant obtained the sum of over $300,000.00 from 10 victims she met via Plenty of Fish, Facebook and Snapchat by concocting various stories in which she was unwell or had bad luck and needed money.[122] In their

[120] [2018] ACTSC 285.
[121] *R v Lancaster* [2018] ACTSC 285, [1] – [2] (Elkaim J); *Criminal Code 2002* (ACT) s 326.
[122] *R v Lancaster* [2018] ACTSC 285, [3] – [4], [37] (Elkaim J).

impact statements, the victims referenced experiencing suicidal ideation and needing significant counselling,[123] feeling heartbroken and emotionally distraught,[124] and feeling "like a puppet and ATM for her".[125] The defendant was sentenced to two years and six months of imprisonment with a 13 month non-parole period.[126]

The case law also demonstrates some unusual circumstances resulting in prosecution of fraud-related offences. In *R v Odbeide*,[127] the defendant, a Nigerian man living in Australia, was involved in a criminal syndicate carrying out online romance scams.[128] He received funds into his bank account from the members carrying out the scams.[129] He used the funds to purchase Bitcoin, pay for daily expenses, and make international transfers.[130] The defendant pleaded guilty to 11 offences in relation to a sum of over $830,000.00,[131] including multiple charges of knowingly or recklessly dealing with proceeds of crime,[132] dealing with property of proceeds of crime,[133] and dealing with identity information to commit an indictable offence.[134] The defendant was sentenced to three years and ten months imprisonment with a non-parole period of two years and one month.[135]

Another unorthodox case is *R v Ferguson*,[136] where a 59-year-old Australian woman, who was the victim of a romance scam, pleaded guilty to three counts of dishonestly obtaining financial advantage by deception.[137] The scammer, who the defendant met on a dating website, claimed to be from Melbourne but unable to meet her due to Covid restrictions.[138] The scammer allegedly travelled overseas for work and claimed that upon his arrival, he was involved in an accident and needed funds.[139] He asserted that the defendant had restricted his access to his bank accounts, thereby manipulating her into feeling financially responsible for him and continuing to send him money.[140] The defendant sent over $1 million to the scammer, the majority of which she took from the club she was employed at as Chief Financial Officer.[141] The defendant received a sentence of three years' imprisonment to be served by an intensive corrections order due to her circumstances.[142] Grant DCJ described the noted the defendant had simply sought happiness on a dating website at a time she was "sad, lonely, depressed and vulnerable",[143] had been victimised by an earlier romance scam involving sextortion,[144] and the shame from being a victim of this romance scam "compounded feelings of low self-worth and confidence resulting from her experience of family violence".[145]

2.1.3 Identity and jurisdiction

Although these three cases go some way to demonstrate the archetypal features of romance scams, the body of case law is few and far between due to various issues involved in prosecuting the scammers. One major issue is ascertaining the identities of scammers. Due to romance scammers strategically using catfish profiles and only speaking to victims online,[146] it is extremely difficult for the police to unmask their true identity and charge

---

[123] Ibid [32].
[124] Ibid [33].
[125] Ibid [34].
[126] Ibid [38].
[127] [2021] NSWDC 750.
[128] *R v Ogbeide* [2021] NSWDC 750, [1], [17] (M L Williams SC DCJ).
[129] Ibid [2], [36].
[130] Ibid [2], [35].
[131] Ibid [7], [10].
[132] *R v Ogbeide* [2021] NSWDC 750, [8] – [9] (M L Williams SC DCJ); *Crimes Act 1900* (NSW) s 193B.
[133] *R v Ogbeide* [2021] NSWDC 750, [1], [17] (M L Williams SC DCJ); *Crimes Act 1900* (NSW) s 193C.
[134] *R v Ogbeide* [2021] NSWDC 750, [1], [17] (M L Williams SC DCJ); *Crimes Act 1900* (NSW) s 192J.
[135] *R v Ogbeide* [2021] NSWDC 750, [66] (M L Williams SC DCJ).
[136] [2022] NSWDC 356.
[137] *R v Ferguson* [2022] NSWDC 356, [5], [12] (Grant DCJ); *Crimes Act 1900* (NSW) s 192E(1)(b).
[138] *R v Ferguson* [2022] NSWDC 356, [15] (Grant DCJ).
[139] Ibid [16].
[140] Ibid [59].
[141] Ibid [18].
[142] Ibid [121], [129].
[143] Ibid [1].
[144] Ibid [59].
[145] Ibid [60].
[146] 'Catfishing' *eSafety Commissioner* (Web Page, No Date) https://www.esafety.gov.au/young-people/catfishing; 'Digital Currencies' *LexisNexis Legal Writer Team* (Practical Guidance AU - Consumer, October 2022) https://advance.lexis.com/document/?pdmfid=1201008&crid=5b0f4a47-6b02-4da1-b782-

them with criminal offences which the police consider can be proved beyond reasonable doubt.[147] Jurisdiction poses another hurdle. Most romance scammers are based overseas and request that the victims' funds are transferred overseas.[148] This introduces various complexities for police investigation and ultimately, police are unable to take substantial actions to prosecute scammers.[149] Cross summarises the identity and jurisdiction issues as follows:

> There are many legitimate reasons why police are not able to investigate cybercrime offences and achieve similar results to offline offences. The inherent lack of borders on the internet poses genuine challenges for police to identify, arrest and prosecute offenders.[150]

2.1.4 Police and private investigators

Despite the identity and jurisdiction issues, there are some examples of police co-operating internationally to take criminal law action against romance scammers. For example, Queensland police have previously worked with the Nigerian government to prosecute 10 Nigerian scammers and return the funds to the victims.[151] More recently, Australian police forces have participated in raids of national call centres suspecting of conducting fraud, including romance scams.[152] The operation, which was codenamed "First Light 2022", saw 76 countries come together to identify global scammers and trigger new investigative leads.[153]

However, police simply do not have the resources or time to investigate the high volume of reports received,[154] and especially not considering the necessary investigations demand coordination with international bodies. Police will only consider following through with an investigation if there are strong prospects of prosecution based on whether the victim's report contains sufficient information regarding the identity and location of the scammer and substantial details of the offence.[155] Even where cases are undefended, police have no duty to recover victims' funds, as they are primarily concerned with convictions.[156]

It follows that the above three cases were likely successful due to the ability to identify the scammers, the scammers being located in Australia and the scammers pleading guilty, which would absolve the police of their burden to prove the offences to the relevant criminal standard. Despite those cases convicting the scammers, there were no orders for the reimbursement of lost funds.

Victims also have the option of instructing private investigators to track down scammers and funds. IFW Global is an organisation of experienced investigators gathering actionable evidence of global scams.[157] Its mission is to provide victims with detailed briefs of evidence to be used for criminal proceedings in relevant

---

491cb5ecea48&pddocfullpath=%2Fshared%2Fdocument%2Fpractical-guidance-au%2Furn%3AcontentItem%3A66PP-PN21-JB7K-206F-00000-00&pdcontentcomponentid=388985&pdteaserkey=sr0&pdicsfeatureid=1517127&pditab=allpods&pddocpracticeareas=urn%3Akrm%3A66E2785780B2443FB43BFFE7BF73E402&ecomp=zdtpk&earg=sr0&prid=b0e4759a-8c6b-454e-980a-f9002d3c33ee&federationidp=MVXHCK52123&cbc=0.

[147] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 116; Gordon Hughes, Suzy Roessel and Jodie Goonawardena, 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.

[148] Aunshul Rege, 'What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud' (2009) 3(3) *International Journal of Cyber Criminology* 494, 506.

[149] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 120 – 1.

[150] Cassandra Cross, 'There's A Gap Between What People Expect When They Report Cybercrime, and What Police Can Deliver' *The Conversation* (Online Article, 18 September 2018) https://theconversation.com/theres-a-gap-between-what-people-expect-when-they-report-cybercrime-and-what-police-can-deliver-102781.

[151] Aunshul Rege, 'What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud' (2009) 3(3) *International Journal of Cyber Criminology* 494, 506.

[152] Australian Competition and Consumer Commission, *Targeting Scams: Report of the ACCC on Scams Activity 2022* (Report, April 2023) 28.

[153] Ibid.

[154] Jessica Lamb, 'Sinister COVID Trend Sees Online Love Scams Target Younger Victims' *ABC News* (online at 11 May 2021) https://www.abc.net.au/news/2021-05-11/covid-love-scams-target-younger-victims/100064644.

[155] Helen Signy, 'Lonely Heart Scams: What Seemed a Genuine Romance Ultimately Left One Woman Devastated' *Australia Reader's Digest* (Blog Post) https://www.readersdigest.com.au/money/lonely-heart-scams.

[156] 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/.

[157] 'About Us: IFW Global' *IFW Global* (Web Page, No Date) https://www.ifwglobal.com/about-us/.

jurisdictions.[158] It does so by leveraging its direct access to local databases, expert witnesses and networks of confidential informants and utilising its strong relationships with state, federal and international law enforcement agencies.[159] However, instructing private investigators is unlikely to be a feasible option for many victims considering their financial losses. Even if the private investigators successfully produce briefs of evidence, it remains up to the discretion of the police to charge the scammers, which they may be unwilling to do for resource reasons.

2.1.5 Victims' expectations

The unfortunate reality of the identity and jurisdiction issues starkly contrasts against victims expectations of the criminal justice system. When reporting romance scams, victims feel that they have been wronged, crimes have been committed and criminal responses are warranted.[160] Such expectations likely come from the media, which suggests it is common for police responses to involve international operations.[161] When met with the reality of what police can deliver, victims become frustrated, angry and dissatisfied with the legal system for not meeting their expectations and serving justice.[162]

2.2 Consumer law

2.2.1 Potential actions against scammers

The ACCC established Scamwatch as the leading organisation helping Australians to identify and avoid scams, and collect reports of scams to help warn the community and take action to stop scams.[163] Scamwatch partners with the eSafety Commissioner ("eSafety"), which an independent regulator supported by the Australian Communications and Media Authority ("ACMA"),[164] and dedicated to working against online risks faced by Australians.[165] Scamwatch is further supported by the Australian Cyber Security Centre ("ACSC") and the Office of the Australian Information Commissioner ("OAIC").[166]

Despite the work of these organisations and in contrast to the criminal law jurisdiction, it is unclear how victims might pursue consumer law actions against scammers to recover lost funds. The most logical basis would be claims of misleading or deceptive conduct pursuant to section 18 of the Australian Consumer Law ("ACL"),[167] although that provision, and many other potentially relevant provisions of the ACL,[168] requires the conduct to occur "in trade or commerce",[169] which "includes any business of professional activity (whether or not carried on for profit)".[170] Romance scams, being private transactions, are effectively excluded from the ambit of the legislation.[171]

---

[158] 'Dating & Romance Scam Investigation' *IFW Global* (Web Page, No Date) https://www.ifwglobal.com/scam/dating-romance-scams/.
[159] Ibid.
[160] Cassandra Cross and Kelly Richards, 'The 'ACA Effect': Examining How Current Affairs Programs Shape Victim Understandings and Responses to Online Fraud' (2015) 27(2) *Current Issues in Criminal Justice* 163, 169.
[161] Ibid 174.
[162] Cassandra Cross, 'Australians Lost $2b to Fraud in 2021. This Figure Should Sound Alarm Bells For the Future' *The Conversation* (Online Article, 6 July 2022) https://theconversation.com/australians-lost-2b-to-fraud-in-2021-this-figure-should-sound-alarm-bells-for-the-future-186459.
[163] 'About Scamwatch' *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/about-scamwatch.
[164] 'Our Structure' *eSafety Commissioner* (Web Page) https://www.esafety.gov.au/about-us/who-we-are/our-structure.
[165] 'Who We Are' *eSafety Commissioner* (Web Page) https://www.esafety.gov.au/about-us/who-we-are.
[166] 'Home' *Scamwatch* (Web Page) https://www.scamwatch.gov.au/.
[167] *Competition and Consumer Act 2010* (NSW) sch 2 s 18.
[168] Eileen Webb, 'Papering Over the Void - Could (or Should) Consumer Law be Used as a Response to Elder Abuse?' (2016) 24 *Competition & Consumer Law Journal* 101, 121.
[169] *Competition and Consumer Act 2010* (NSW) sch 2 s 18.
[170] Ibid sch 2 s 2.
[171] Eileen Webb, 'Papering Over the Void - Could (or Should) Consumer Law be Used as a Response to Elder Abuse?' (2016) 24 *Competition & Consumer Law Journal* 101, 121.

Alternatively, victims may pursue civil fraud actions against scammers. Solicitors of Davies Collison Cave suggest that the tort of deceit may be available to victims.[172] The tort of deceit may be established if the victim can prove on the balance of probabilities that the scammer made a false representation, the scammer did so with the knowledge that it was false and intention that the victim would rely on it, and the victim relied on the representation and consequently suffered damage.[173] In *Magill v Magill*,[174] the majority judgment found there is scope for the tort to apply to certain situations between romantic partners.[175] This suggests the tort could extend to apply to romance scams if victims claim their communications with scammers are false representations.

2.2.2 Discovery orders

Much like the criminal law responses, consumer law actions are dependent on identifying and locating the scammers.[176] As established, scammers rely on fake identities and jurisdictional divides, therefore making it notoriously difficult to commence consumer law proceedings against scammers.[177] In this event, victims could attempt to identify and locate scammers by applying to the appropriate court for a discovery order to ascertain the scammer's identity or location pursuant to rule 5.2 of the *Uniform Civil Procedure Rules,*[178] or the equivalent in other states. Discovery orders can compel banks, internet providers and/or other relevant third parties to disclose information which may assist in ascertaining a scammer's identity and location.[179] Specialist fraud law firms such as Duxton Hill offer services to obtain such orders.[180]

However, discovery orders are only available after victims have made reasonable enquiries to identify and locate the scammer.[181] Victims may expect their banks to share scammers' identities to assist them in pursing actions, however for privacy reasons, banks will not disclose the details of recipients unless ordered to do so by a court.[182] These conditions place the onus on victims to make initial enquiries and then pursue discovery orders,[183] merely to have a chance of ascertaining the scammer, who is likely hiding behind several layers of anonymity through the use of sophisticated technology.[184] At a time of heightened emotional turmoil and in the wake of financial loss, most victims are likely focused on simply managing their own welfare and will treat any additional legal burdens as a secondary priority,[185] if at all, considering the majority of victims do not commence proceedings.[186] Overall, victims of romance scams are often unable to recover lost funds directly from scammers.[187]

---

[172] 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[173] *Magill v Magill* [2006] 226 CLR 551, [114] (Gummow, Kirby and Crennan JJ).
[174] [2006] 226 CLR 551.
[175] *Magill v Magill* [2006] 226 CLR 551, [129] (Gummow, Kirby and Crennan JJ).
[176] 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[177] Marilyn Krawitz, 'Stop! In the Name of Fraud, Before You Break Your Bank Account: Actions to Take When Your Client is the Victim of Online Dating Fraud' (2013) 16(3) *Internet Law Bulletin* 75, 75 – 6.
[178] *2005* (NSW).
[179] *Uniform Civil Procedure Rules 2005* (NSW) r 5.2; 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/.
[180] 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/.
[181] *Uniform Civil Procedure Rules 2005* (NSW) r 5.2.
[182] 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/.
[183] 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[184] Ibid.
[185] Eileen Webb, 'Papering Over the Void - Could (or Should) Consumer Law be Used as a Response to Elder Abuse?' (2016) 24 *Competition & Consumer Law Journal* 101, 124.
[186] 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[187] Ibid.

Further, in *Deputy Commissioner of Taxation v Shi,*[188] Gordon J explained that any information obtained about a potential defendant through a discovery order cannot also be used in criminal proceedings against the potential defendant unless a court grants leave to do so.[189] Leave may be granted in "special circumstances",[190] including "most importantly of all, the likely contribution of the [information] in achieving justice in the [criminal] proceeding".[191] This loads yet another procedural burden on to victims seeking to collate briefs of evidence for the police to consider actioning.

2.2.3 Liability of banks

One practicable alternative is to request assistance from their banks that facilitated the payment, however whether the banks are willing to compensate victims is usually left to the banks' discretion.[192] Banks have some responsibilities regarding unauthorised transactions and mistaken payments, are obliged to comply with the terms and conditions of the account as well as the Australian Banking Association ("ABA") Code of Practice, and are subject to ACL and relevant contract law and other common law.[193] Despite these various obligations, there are limited situations where banks are liable to pay victims for the funds lost during romance scams.[194] Liability is dependent on how aware the bank was of the scam and what role they played in the transaction.[195] For example, if the bank had received prior complaints or ASIC notifications of an account engaging in fraudulent transactions and failed to close that account before a particular romance scam occurred, then the bank has a degree of culpability in the scam and arguably should take some responsibility.[196]

Unsurprisingly, in the majority of cases, victims have authorised transactions to scammers.[197] Banks perceive the authorisations as negating their liability and continue to push the onus for stopping scams onto consumers.[198] Banks may contact scammers to request the funds be returned, but this is usually the limit of their involvement.[199] Many victims lodge complaints with the Australian Financial Complaints Authority ("AFCA"), however only 5% of cases result in favourable outcomes for victims.[200]

It follows that a debate has emerged between consumer law advocates and banks as to whether the latter should be covering reimbursements to scam victims.[201] One regulator in the United Kingdom proposed a plan to mandate banks reimbursing victims of a particular scam whereby scammers were asking victims to pay by bank transfers.[202] Gerard Brody, former Chief Executive Officer of the Consumer Law Action Centre and current board member at ACFA, advocates for a similar reform in Australia to address the lack of consistency for how banks response to scam victims, explaining:

> There should be a standard, and if [banks] don't meet it, they should be reimbursing customers.[203]

Arguably, a mandatory commitment to reimbursements would incentivise banks to take meaningful action

---

[188] (2021) 392 ALR 1, [50] (Gordon J).
[189] *Deputy Commissioner of Taxation v Shi* (2021) 392 ALR 1, [50] (Gordon J).
[190] Ibid.
[191] *Liberty Funding Pty Ltd v Phoenix Capital Pty Ltd* (2005) 218 ALR 283, [31] (Branson, Sundberg and Allsop JJ).
[192] 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[193] 'Scams' *Financial Rights Legal Centre* (Web Page, January 2023) https://financialrights.org.au/factsheet/scams/.
[194] Ibid.
[195] Ibid.
[196] Ibid.
[197] 'Opinion: Banks, Get Tougher on Scams' *Consumer Action Law Centre* (Blog Post, 18 February 2023) https://consumeraction.org.au/opinion-banks-get-tougher-on-scams/.
[198] 'Romance Scams', *Duxton Hill* (Web Page) https://duxtonhill.com.au/romance-scams/.
[199] Ibid.
[200] 'Opinion: Banks, Get Tougher on Scams' *Consumer Action Law Centre* (Blog Post, 18 February 2023) https://consumeraction.org.au/opinion-banks-get-tougher-on-scams/.
[201] Clancy Yeates, 'Scam Losses Could Hit $4b This Year. Should Banks Wear the Cost?' *Sydney Morning Herald* (Blog Post, 9 November 2022) https://www.smh.com.au/money/planning-and-budgeting/scam-losses-could-hit-4b-this-year-should-banks-wear-the-cost-20221107-p5bw9p.html.
[202] Ibid.
[203] Ibid.

against scammers.[204] Not only would this better position victims to receive relief where often there are no other viable options to do so, but the new standards would also be advantageous from a business management perspective, as better protection systems would lead to lower rates of scams and less expenditure on complaints handling.[205]

Unsurprisingly, banks disagree with the calls. A spokesperson for the ABA claims banks often cover losses to scammers, including the sum of $103 million in losses in the 2020–21 financial year.[206] However, banks will not take responsibility where victims have been warned about particular risky transactions and proceed anyway.[207] The ABA spokesperson elaborated:

> Proposals for schemes which require banks to cover customer losses do not adequately take into account the incentive this provides financial criminals or scammers to target Australians.[208]

Assistant Treasurer and Minister for Financial Services, Stephen Jones, shares a similar perspective, explaining that banks always reimbursing victims irrespective of the circumstances would create a "honey pot" for scammers and raise the appeal of scamming Australians.[209]

3 Prevention and intervention

Although there is some scope for criminal and consumer law responses to apply to romance scams, those applications are plagued with uncertainties and complexities. Instead, there appears to be a growing focus on the prevention and intervention of scams.[210] In an April 2023 media release, Catriona Lowe, current Deputy Chair of the ACCC, outlined the main challenge Scamwatch faces and the three-pronged approach it continues to advocate:

> Unfortunately, there are still significant gaps between and within the key sectors - banks, telcos and digital platforms; and between regulators that scammers exploit to steal money from consumers. So we would like to see initiatives that apply across the sectors, knowing that scammers will target the weakest link.
>
> …
>
> First, we need to stop scammers reaching consumers by disrupting phone calls, SMS, email, social media messaging or other ways in which scammers contact would-be victims. Second, we need to make sure consumers are supported with up-to-date information so they have the best chance of spotting a scammer when contacted. Finally, we need effective measures in place to prevent funds being transferred to scammers.[211]

Other relevant bodies appear to support the focus on preventing and intervening romance scams. Chris Goldsmid, the AFP Commander of Cybercrimes Operations, highlights scammers are more cunning than ever

---

[204] 'Opinion: Banks, Get Tougher on Scams' *Consumer Action Law Centre* (Blog Post, 18 February 2023) https://consumeraction.org.au/opinion-banks-get-tougher-on-scams/.
[205] Ibid.
[206] Clancy Yeates, 'Scam Losses Could Hit $4b This Year. Should Banks Wear the Cost?' *Sydney Morning Herald* (Blog Post, 9 November 2022) https://www.smh.com.au/money/planning-and-budgeting/scam-losses-could-hit-4b-this-year-should-banks-wear-the-cost-20221107-p5bw9p.html.
[207] Ibid.
[208] Ibid.
[209] Ibid.
[210] Gregor Urbas, *Cybercrime: Legislation, Cases and Commentary* (LexisNexis Butterworths Australia, 2015) 110.
[211] Australian Competition and Consumer Commission, 'ACCC Calls for United Front as Scammers Steal Over $3bn from Australians' (Media Release, 17 April 2023).

and suggests individuals and organisations face extreme difficulty in identifying the scams.[212] Cross has stated that this approach is "key to making any inroads in reducing losses".[213]

In light of the above, this remainder of the paper will critically discuss how Scamwatch and related organisations are currently focusing on prevention via community education and awareness and intervention by way of third party regulations.

3.1 Prevention: community education and awareness

Although it is almost impossible to prevent romance scammers from contacting victims in the first place,[214] scammers are undoubtedly less likely to succeed if their targets have heard about the scams prior to being targeted.[215] Similar to Lowe, Julie Inman Grant, eSafety Commissioner, explains the key role of community awareness and education:

> The best way to defeat scammers is by equipping all Australians with the skills to recognise this predatory online behaviour before it's too late, by raising awareness of the dangers and educating people about how to avoid them.[216]

Scamwatch runs an awareness-raising campaign,[217] which Urbas has described as "promising" as it aims to alert potential victims to the reality of the scams.[218] The campaign encompasses a range of romance-specific resources, including media releases, example transcripts, real life stories, statistics, infographics and fact sheets, news and alerts publications,[219] and it is further supported by references to romance scams in general resources such as YouTube videos, annual reports, The Little Black Book of Scams and the initiatives of the Scams Awareness Network, such as Scams Awareness Week.[220]

One example of the campaign is the main Scamwatch romance scams web page which, in addition to outlining how the scams work and who to contact about the scams, equips potential victims with a list of warning signs and self-protection tips which are extracted below:[221]

Warning signs it might be a scam	**Steps you can take to protect yourself**

[212] Australian Federal Police, 'When Love Hurts: A Warning to Lonely Hearts' (Media Release, 14 February 2023).
[213] Cassandra Cross, 'Australians Lost $2b to Fraud in 2021. This Figure Should Sound Alarm Bells For the Future' *The Conversation* (Online Article, 6 July 2022) https://theconversation.com/australians-lost-2b-to-fraud-in-2021-this-figure-should-sound-alarm-bells-for-the-future-186459.
[214] Gordon Hughes, Suzy Roessel and Jodie Goonawardena, 'Australia: COVID Scams: The Catalyst for Law Reform?' *Mondaq* (Blog Post, 2 February 2022) https://www.mondaq.com/australia/white-collar-crime-anti-corruption-fraud/1156930/covid-scams-the-catalyst-for-law-reform.
[215] Monica Whitty and Tom Buchanan, 'The Online Romance Scam: A Serious Cybercrime' (2012) 15(3) *Cyberpsychology, Behavior and Social Networking* 181, 181.
[216] Bianca Iovino, 'Older Man the Latest Victim in Dating Scam, Days Out From Valentine's Day' *Hellocare* (Blog Post, 8 February 2023) https://hellocare.com.au/older-man-the-latest-victim-in-dating-scam-days-out-from-valentines-day/.
[217] 'Be Alert for Romance Scams this Valentine's Day' *Australian Banking Association* (News and Resources, 14 February 2023) https://www.ausbanking.org.au/be-alert-for-romance-scams-this-valentines-day/.
[218] Sharon Givoni, 'Interview with Dr Gregor Urbas, Author of Cybercrime: Legislation, Cases and Commentary, 2nd edn' (2022) 24(9) *LexisNexis Internet Law Bulletin* 162, 166.
[219] 'Search' *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/search?query=romance+scams.
[220] 'Research and Resources' *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/research-and-resources.
[221] 'Romance Scams', *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/types-of-scams/dating-romance.

• They express strong feelings quickly and the relationship moves fast. You are made to feel special quickly. • If you are chatting on your usual social media platform or an official dating service, they will quickly try and move the conversation offsite, for example to WhatsApp. • Romance scammers will encourage secrecy and will influence you to only trust them. They may try to isolate you from your family and friends. • There will always be an excuse why they can't meet in person or show themselves on camera. They say they live overseas or somewhere remote, or their technology isn't working. • Their online profile doesn't match what they tell you about themselves. • They talk about money or investments. They might say they know about cryptocurrency and offer to teach you. • You are asked for personal photos, videos or information they could use against you in the future. • The scammer gets desperate or angry if you don't do what they ask. They may threaten to cut off the relationship.	Never send or transfer money to someone you haven't met • If your online connection asks you for money, they are likely a scammer. Stop contact right away and seek support. • Don't send money, card or bank details or important identity documents like your passport to someone you've only met online: no matter how long you've been messaging them. • Never agree to transfer money for someone else. It's called money laundering and being involved is a criminal offence. Check the person is who they say they are • Take things slowly. Ask lots of questions and watch for things that don't add up. • Search for the scammer's name along with the word "scam" in a search, and look for websites about romance scams in the results. Be careful what you share (and what you don't) • Never send intimate pictures or videos of yourself to people you don't know. Scammers use these to blackmail people. • Don't keep your online relationship a secret. Speak to people you know about it. It can be easier for others to spot the warning signs. • Be careful about what you share about yourself online. Scammers can use information about your hobbies, job or family to target you. • Find out more about how to stay safe on different social media platforms [on the eSafety Commissioner website]. Learn how to spot a fake profile • Photos that look too professional. • Very little personal information. • No connection to social media accounts. • Few comments, likes or shares on their social media from other people.

Promoting the above signs and tips is a practical and effective way of cutting through romantic facades and aiding potential victims to trust the negative gut feelings that many of them have when their online partner first asks them for money.[222] The inclusion of specific references to cryptocurrency, money laundering, sextortion and identity fraud helps alert potential victims that these niches may be mixed in with romance scams. The language used is simple and assertive in directing potential victims how to act against romance scams, yet the underlying tone appears understanding and sympathetic of the context in which the scams occur. The message softens the long-standing shame and stigma surrounding romance scam victims and effectively creates a basis for societal discourse to openly and constructively discuss the scams.[223] The ACCC's campaigning is solidified

[222] Griffiths News, 'Romance Scams - Anyone Can Fall Victim', *Griffith University* (Blog Post, 7 February 2018) https://news.griffith.edu.au/2018/02/07/romance-scams-anyone-can-fall-victim/.
[223] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 3.

by similar advocacy undertaken by other relevant organisations, including the ABA,[224] Match Group, which owns dating platforms Tinder, Hinge and Plenty of Fish,[225] and the eSafety Commissioner.[226]

Urbas praises awareness and education campaigning for enabling concerned families and friends to obtain support for potential victims.[227] For example, the ACCC has a web page aimed to assist individuals identify scams and seek assistance on behalf of their loved ones.[228] That web page also highlights the vulnerabilities of victims and the effects that scams have on their wellbeing, and encourages individuals to remain patient, supportive and cognisant of their loved ones' circumstances.[229]

In a recent news publication, Lowe urged Australians to have calm and gentle conversations with their loved ones to help them recognise the warning signs, such as asking about the nature of the relationship and why they have not been able to video chat or meet in person.[230] Drew also gave individuals advice on how to appropriately support potential victims, from giving them time and space to discuss the relationship over multiple conversations through to ensuring the support continues while they grieve the relationship and rebuild self-esteem.[231] Campaigning to the community is absolutely crucial to preventing romance scams from occurring because, even if exposed to campaign material, many potential victims will perceive their relationship as being genuine and "the exception" to any warnings.[232] Lowe has confirmed that a significant proportion of reports to the ACCC come from families and friends.[233]

Although the current awareness and education campaigning is meritorious, there are certainly a few key areas for improvement. Firstly, the ACCC should amend its current messaging by reframing advice for victims not to contact people they "don't know" to people they "have not met".[234] Victims perceive they are not sending money to strangers but to their online connections, so reframing the advice could more effectively assist victims to identify their partners as scammers.[235]
Further, the community would benefit from resources targeted to each of the especially susceptible demographics.[236] For example, the ACCC has translated The Little Black Book of Scams into ten languages,[237] and the eSafety Commissioner has developed a range of anti-scam resources for vulnerable community

---

[224] 'Be Alert for Romance Scams This Valentine's Day' *Australian Banking Association* (Blog Post, 14 February 2023) https://www.ausbanking.org.au/be-alert-for-romance-scams-this-valentines-day/.
[225] Nicola Field, 'Romance Scams: It's Not Love, Actually', *Money* (Blog Post, 19 April 2023) https://www.moneymag.com.au/how-to-spot-a-romance-scam.
[226] 'Online Scams' *eSafety Commissioner* (Web Page) https://www.esafety.gov.au/key-issues/staying-safe/online-scams.
[227] Sharon Givoni, 'Interview with Dr Gregor Urbas, Author of Cybercrime: Legislation, Cases and Commentary, 2nd edn' (2022) 24(9) *LexisNexis Internet Law Bulletin* 162, 166.
[228] 'Help Someone Who's Being Scammed' *Australian Competition and Consumer Commission Scamwatch* (Web Page) https://www.scamwatch.gov.au/protect-yourself/help-someone-whos-being-scammed.
[229] Ibid.
[230] Australian Competition and Consumer Commission, 'Have a Heart-to-Heart With Loved Ones to Help Stop Scams This Valentine's Day' (Media Release 8/23, 12 February 2023).
[231] Danielle Maguire and Nicholas McElroy, 'Think Your Relative is Caught Up in a Romance Scam? Here's How to Talk to Them About Love Scams This Valentine's Day' *ABC News* (online at 14 February 2023) https://www.abc.net.au/news/2023-02-14/romance-scams-how-to-help-online-dating-valentines-day/101959558.
[232] Michael Deacon, 'Bytes: There's Nothing Romantic About Online Fraud' (2010) 13(2) *LexisNexis Internet Law Bulletin* 40, 41.
[233] Jessica Yun, 'Sextortion and 'Very Expensive Heartbreak': Beware Valentine's Day Scams, says ACCC' *The Sydney Morning Herald* (online at 14 February 2023) https://www.smh.com.au/business/consumer-affairs/sextortion-and-very-expensive-heartbreak-beware-valentine-s-day-scams-says-accc-20230212-p5cjuk.html.
[234] Queensland University of Technology, *Centre for Justice Briefing Paper: A Guide to Understanding Romance Fraud* (Briefing Paper Issue No 22, February 2021) 3.
[235] Ibid.
[236] Cassandra Cross, 'Australians Lost $2b to Fraud in 2021. This Figure Should Sound Alarm Bells For the Future' *The Conversation* (Online Article, 6 July 2022) https://theconversation.com/australians-lost-2b-to-fraud-in-2021-this-figure-should-sound-alarm-bells-for-the-future-186459.
[237] Australian Competition and Consumer Commission, *The Little Black Book of Scams* (Guide, July 2023) https://www.scamwatch.gov.au/system/files/The%20Little%20Black%20Book%20of%20Scams%20-%20July%202023%20-%20Web.pdf.

groups.[238] Combining these types of initiatives to develop tailored resources to each community group could improve effectiveness.[239]

Finally, the ACCC should take steps to ensure consumer and competition lawyers possess the appropriate knowledge to identify clients who may be potential victims of romance scams, such as knowing to tactfully ask further questions if clients ask about the best way to transfer money abroad or taxation implications with doing or ask about the legal consequences of receiving money from someone overseas or transferring money to someone else overseas, and knowing to alert client to the possibility of romance scams.[240]

- Fraud takes human approach - seek to capitalise on victims' weaknesses in calculated manner - shift focus to counteract fraud prevention messages to public from police and other agencies - e.g ACCC Little Black Book of Scams 2008 - comprehensive details of common fraud schemes - to counter messaging - offenders recruit Australians to launder funds - known as money mules - often victims themselves - asked to receive and transfer money on behalf of offenders - fewer red flags when asked to send money to Big Four bank account in Melbourne compared to Lagos
- Advantages to consumer protection approach - regulators already on lookout for such conduct - if several matters come to attention of regulator, could take matters forward rather than individual older people trying to navigate process - some matters resolved more efficiently than present - suggestion various hierarchies should be reviewed to enable matters to be brought to various consumer tribunals - presence of regulator sends unambiguous message to persons engaged in conduct targeting older people - one individual matter may go unnoticed however profile of regulator can use actions to address conduct and highlight issue through education and awareness strategies - involvement puts financial institutions on notice re elder abuse issues - 126

3.2 Intervention: third party regulations

As alluded to above, the ACCC is undeniably pushing for third parties facilitating romance scams to be subject to regulations compelling them to intervene in the scams.[241] In the case of dating and social media apps, this would involve disrupting communications between scammers and victims.[242] Banks and other financial institutions would be expected to stop funds from being transferred to scammers.[243]

- Greater recognition of problem across government and industry - still sense of shame and embarrassment at being deceived - victims have difficulty reporting

Banks

- Queensland 80 year old man about to send $20,0000 to scammer when Bank of Queensland intercepted transaction due to suspicion being scammed
- CBA recently introduced two new measures to prevent scams
- CBA launching new verification measures for money transfer and phone banking
- Australian Financial Complaints Authority chief executive David Locke - "we see every day, in our work with consumers and banks, the devastating impact scams can have on people. We welcome any initiatives by banks to seek to protect their customers, including the innovative use of technology."
- Banks need to urgently invest in better systems and technology to stop scammers in their tracks - e.g CBA introducing NameCheck technology to online payments in March - aimed at limiting ability of scammers to issue false invoices - vital all banks follow suit
- Jan Santiago deputy director Global Anti-Scam Organisation - "we make financial innovation so easy, and

---

[238] 'Helping Australians Have Safer and More Positive Experiences Online' *eSafety Commissioner* (Web Page) https://www.esafety.gov.au/.
[239] Cassandra Cross, 'Australians Lost $2b to Fraud in 2021. This Figure Should Sound Alarm Bells For the Future' *The Conversation* (Online Article, 6 July 2022) https://theconversation.com/australians-lost-2b-to-fraud-in-2021-this-figure-should-sound-alarm-bells-for-the-future-186459.
[240] Marilyn Krawitz, 'Stop! In the Name of Fraud, Before You Break Your Bank Account: Actions to Take When Your Client is the Victim of Online Dating Fraud' (2013) 16(3) *Internet Law Bulletin* 75, 76.
[241] Australian Competition and Consumer Commission, 'ACCC Calls for United Front as Scammers Steal Over $3bn from Australians' (Media Release, 17 April 2023).
[242] Ibid.
[243] Ibid.

social engineering has led to less point-of-contact. [Digital financial services] should have the protection afforded as if a person goes into a bank physically and talks to a bank teller."
- Alma Angotti partner at Guidehouse - consumer education is key for financial institutions to be able to prevent and detect frauds - especially when payments often not large - financial institutions not necessarily able to identify fraud because it may look like an unremarkable payment - crypto trading platforms have responsibility to make sure users know how crypto works
- Stricter know-your-customer onboarding processes and improved fraud detection at trading platforms and banks
- Banks and financial institutions need to implement measures to help reduce fraud losses - including checking account names against BSB numbers for all transactions - UK has confirmation of payee policy that does this - https://www.ukfinance.org.uk/policy-and-guidance/guidance/confirmation-payee
- Crypto by nature is global and decentralised - payments made outside of Australia - prevention is easier than cure - know who dealing with, transact through reputable exchange, ensure all channels verified
- Australia crypto exchanges must be registered through AUSTRAC in compliance with anti-money laundering and counter-terror financing obligations - currently no licensing requirements - e.g capital requirements or cybersecurity
- Last year - Senate Select Committee into Australia as Technology and Financial Centre recommended more comprehensive licensing framework - Australian government agreed with recommendation - federal treasury department due to consult on what this will look like

R v Ogbeide [2021] NSWDC 750 M L Williams SC DCJ
[42] It was clearly a money laundering syndicate with a high degree of sophistication. Members of the syndicate used a number of means to conceal the source of the proceeds received from the commission of the frauds, they used numerous account holders, used handlers to recruit and communicate with the account mules and shortly after the money was deposited into an account holder's account it was used to purchase either gold bullion or foreign currency with smaller amounts withdrawn in cash. The syndicate sent proceeds to Nigeria using a number of means, including Bitcoin and members of the syndicate communicated through numerous encrypted services including WhatsApp, Signal and Snapchat.

- Authorities need to employ new methods of protection - regulations currently applying to financial advice and products to be extended to crypto - data scientists need to better track and trace fraudulent activities
- However convincing case for pushing banks and other business to beef up anti-scam defences in other ways - e.g ACCC called for banks to improve systems designed to spot payments to scammers - Jones has promised to introduce tough new industry codes for banks, telcos and social media platforms to reduce economic crime - codes need to have meaningful consequences for businesses not complying to be impactful on growing wave of online scams

ABA argues for sustained effort from government bodies, telcos, online shopping platforms, public - working on developing consistent industry position and encourage people to use PayID allows payer to see who paying before sending money -

Police
- WA victim found dead in rented villa - travelled to South Africa to visit Nigerian man - 67 year old widow Jette Jacobs - left WA 22 November 2012 - body found Johannesburg 9 February 2013 - investigated by local police - WA police believe suspicious circumstances - money, credit cards, jewellery, laptop missing from villa - lost partners in 2002 and 2009 - met Jesse Orowo Omokoh from Nigeia on dating website - four year relationship - sent at least $80,000 to Nigeria - met Jesse in Johannesburg in 2010 without incident - during last visit was to meet Jesse again but he said he couldn't get visa to join her - letter from Project Sunbird sent warning may be victim of fraud but arrived after she left Australia - joint project between WA Police and Consumer Protection tracks large sums of money being sent from WA to Western African countries - attempts to warn senders they could be victims - Detective Senior Sergeant Dom Blackshaw of Major Fraud Squad WA Police said evidence Jesse arrived two days before reporting death and giving statement to local police - "during Project Sunbird, we were alarmed to discover that some fraud victims had plans to visit their interent partners in Africa. An Albany man was about to leave for Africa when we interened and another woman oin the south west of the State aksi stated that she had booked her flight but luckily changed her mind at the last minute. These relationship frauds are being perpetrated by ruthless overseas criminal who are members of organsied crime syndicates. To travel to Africa to visit someone you have met on the internet is extremely dangerous and could,

as in the case of Ms Jacobs, cost your life." - Google WA ScamNet 'Death of WA Romance Fraud Victim' - main suspect arrested in Nigeria in June 2014 and charged with nine counts of conspiracy and obtaining money by false pretences - 107

- AFP "fifteen Australians, who thought they had found love, were identified as being money mules under a national anti-money laundering campaign"
- 15 Australians – thought found love – used as money mules – transfer illicit money on behalf of someone else – usually members of criminal syndicates
- Campaign in conjunction with Europol's eight annual global anti-money mule operation – known as European Money Mule Action 8 – 2469 arrests around world – 21 in Australia
- Accused of dealing in proceeds of crime
- Police intervened in these instances involving innocent victims – people who are knowingly complicit in illegal schemes face serious penalties – jail for up to 25 years
- AFP prevented woman from losing $50,000 to boyfriend scammer – WA authorities intercepted package of money before sent to another Australian state – AFP spoke to woman – said her boyfriend needed money to pay workers until he could free up cash – conversations made it clear it was scam – ongoing investigations into identity
- QPS informed Committee of two operations - Operation Echo Track and Operation Hotel fortress - gather info on victims of advance fee fraud including romance scams - 47
- Knowledge of romance scam not necessarily translating into protective actions - QPS informed Committee 76% of victims who lost large amounts of money continued to willingly participate in such scams despite being notified by QPS they were being victimised - 58
- Peter Shenwun Consular Minister Nigerian High Commission in Australia told Committee many victims of advance-fee fraud originating out of Nigeria seek to continue contact with scammers despite being advised not to by Nigerian authorities - 58
- Example - Operation Sunbird in WA - joint initiative between Western Australian Department of Commerce and Western Australian Police Major Fraud Squad - letters sent to potential victims to stop sending money and contact consumer protection for further advice and assistance - 4708 letters sent - 67% were first contacts with potential victims - letters disrupted transfer of money from WA to romance scammers in Africa - 115

- Victims would like to see more determined effort from federal authorities – track and shut down criminal syndicates – Australian Cyber Security Centre directed to NSW Police – police did not have resources at local detective level to mount international investigation

PROJECT SUNBIRD
- Analyse financial intelligence data and remove non-fraudulent money transfers
- Those left identified as possible fraud victims - usually victims of romance scams - letter to householder notifies person likely caught up in fraud - about 60% stop sending after first letter - continuing to send funds - more detailed second letter sent direct to person sending funds - about 40% stop
- Sent to more than 1965 people - combined loss $9.5 million reported by over 150 people
- One-on-one proof its a scam sessions between victims and police
- Background disruption - shutting down scammer email and social media accounts - investigation activity to look at web of false identities used - where wire transfers collected and dodgy bank accounts at centre of fraud
- New initiative in 2014 - detectives from Nigeria's Economic and Financial Crimes Commission come to WA to work collaboratively with on cases involving Nigerian suspects - resulted in arrests re romance frauds targeting WA
- Project Sunbird successful - monitored by other states and territories - may be mirrored elsewhere in Australia

Dating apps
- follows introduction of new app features including selfie verification and pop-up messages with safety tips if certain language detected in conversations
- Buddy Loomis senior director of law enforcement operations and investigations at Match Group - believes leveraging technology and resources helps users make safer online connections - still user-beware environment
- Dating apps have more protections than different chat sites – e.g remove profile if reported – protects other people
- University of Queensland researcher Madeleine Taylor – studied more than 100 dating websites and apps in

Australia and the corporate responsibility of companies to protect their consumers from scammers – Bumble, Tinder, E-Harmony – getting better at scam-proofing their platforms – use of photo and face recognition – "Bumble does it and Tinder has started a trial in the US using photo recognition, where you upload a photo and they get you to take a live photo of yourself doing a specific pose. They can verify that you are a real person and the testimonial photo is yours; that's a really valuable tool for websites to implement. It's completely an ethical and discretionary responsibility; there's nothing in our legislation that suggests they have to do this. And the guidelines are completely voluntary, so there is very little accountability or actual responsibility for them to implement these measures." – re companies have no legal obligation to use protection measures on their platforms, but it benefitted their users and made them feel safer online

4 The National Anti-Scam Centre

ALP proposal
- NASC - coordinate efforts of several industry and enforcement entities responsible for preventing and remedying scams - bring together law enforcement, banks, telecom providers, consumer advocates - allow real-time information sharing to better protect consumers
- Additional funding for ID recovery services, new industry code for industry and government to clearly define responsibilities re protecting consumer, measures to ensure companies do not profit from fraud on platforms
- Calls for telecoms and banks to change way communicate with customers to avoid consumers falling prey to scams
- Referred to UK Fusion Cell and Canada Anti-Fraud Centre - examples of foreign governments successfully implementing similar systems - although elements of UK being overhauled including to respond to reported trust issues re info sharing and Canada initiatives came into effect only recently and appear to mirror ScamWatch and ReportCyber

Next steps
- Unclear whether plan would bring tangible change - but clearly action needed - current frameworks offer almost nothing to prevent scammers from making endless unwanted contact and offer very little to those suffered loss - where scammer cannot be identified (usually case) - near impossible to recover losses or reprimand scammer
- Instead onus on individuals to better inform themselves and avoid falling prey - expected to live with it

- Government attempting to address continued surge in fraud losses through revision of cybersecurity strategy and potential establishment of National Anti-Scams Centre - positive steps but more needs to be done

- October 2022 - Federal Government announced allocation of seed funding to ACCC for establishment of National Anti-Scams Centre
- ACCC to consult and engage with key stakeholders - including NASC survey
- Seeking input on what NASC functions and role - facilitate real time collaboration with stakeholders who have existing responsibilities for anti-scam work including models and governance frameworks and other related issues
- Will continue engagement with stakeholders

- Human problem - need to better understand psychological techniques used by offenders and develop targeted ways to fight back
- Time government took fraud more seriously - invest resources and expertise into reducing losses - currently no coordinated fraud strategy to mitigate, prevent or respond to losses
- Clear need to develop better education and prevention materials accounting for diversity in victimisation - knowing certain demographics more likely to be victimised highlights need to create tailored resources

- October budget (2022?) – seed funding from government to scope and plan new National Anti-Scams Centre to support community fight against scams
- Recent federal budget - $9.9 million over four years for National Anti-Scam Centre to coordinate work of different agencies
- Day – "What we expect through the work and the cooperation that will come through that NASC is that we are going to start to see these things go down"

- Early November 2021 - Australian Labour Party pledged to establish National Anti-Scam Centre - would bring together key industry and enforcement entities with aim of better protecting Australian consumers - is Centre what we're missing? - what protections are already in place and why not working?

"As scammers become increasingly sophisticated in their tactics, it is clear a coordinated response across government, law enforcement and the private sector is essential to combat scams more effectively."

"That's why we continue to lend our expertise and support to prepare for the establishment of the Government's National Anti-Scam Centre, with the ultimate aim of making Australia the hardest target for scammers," Ms Lowe said.

Conclusion

that the most appropriate and effective response of the scams is to focus on prevention and intervention initiatives, and that part of the role of the NASC must be prioritising the improvement and maintenance of such initiatives, as well as the secondary focus of developing criminal and consumer responses if and where possible.