TINDER SWINDLERS: SUBSTANTIVE AND PROCEDURAL MATTERS PERTAINING TO ONLINE DATING FRAUD UNDER THE COMMON LAW AND THE CYBERCRIMES ACT

Delano Cole van der Linde
LLB LLM LLD
Senior Lecturer, Stellenbosch University

SUMMARY

The proliferation of online dating scams or fraud has presented a significant threat to users of online dating platforms globally. Scammers misrepresent themselves as would-be lovers, usually employing false identities, in order to defraud unsuspecting victims of large sums of money. Not only do romance scammers cause great financial harm to their victims, but also often leave victims with long-term psychological scars. As both the common law and the Cybercrimes Act 19 of 2020 address instances of fraud, both may potentially be employed to address the issue of online dating fraud. The State may charge an accused with both offences, but a conviction based on both would probably constitute a duplication of convictions. The offence of cyber fraud under the Cybercrimes Act may however be more onerous to prove, owing to the particular way that cyber fraud must be committed under section 8. A conviction based on the Cybercrimes Act may, however, be more attractive to the State as certain minimum sentences apply, depending on the amount defrauded, whether the accused was a law enforcement officer, whether someone was in charge of or had access to the data belonging to others, and whether the offence was committed in concert with others.

1 INTRODUCTION

In her ballad, *Think Twice*, Celine Dion once famously sang, "Don't think I can't feel that there's something wrong."[1] This line resonates well with many in the age of online dating, which has left numerous users as victims of a romance scam. In broad terms, romance scams involve fraudsters using fake profiles (or "catfishing") to seduce victims on dating websites and mobile applications (apps) such as Tinder, with the eventual goal of conning them out of a sum of money. The United States Federal Trade Commission (FTC) recently reported that it had received over 70 000 complaints of romance scams during 2022, totalling an estimated $1.3 billion

[1] Dion "Think Twice" *The Colour of My Love* (1993) (© Sony Music Entertainment).

(approximately R24 billion).[2] It confirmed that the median loss incurred by victims was approximately $4 400 (approximately R81 000).[3] The proliferation of online dating sites[4] and dating applications has therefore created a corresponding risk of fraud.[5] Although no empirical evidence of the financial implications of cyber romance scams seems to exist in South Africa, it is clear that cyber fraud in general is quite pervasive.[6]

There has been an attempt to address cybercrime broadly at the regional and national levels. An underlying theme is a call for harmonisation and coordination of legislative instruments to combat cybercrime. These instruments, which include the Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (Model Law),[7] the African Union Convention on Cyber Security and Personal Data Protection[8] (AU Convention),[9] and the Council of Europe's Convention on Cybercrime[10] (Budapest Convention),[11] all call for the criminalisation of cyber fraud.[12]

---

2 Fletcher "Romance Scammers' Favorite Lies Exposed" (9 February 2023) https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft1 (accessed 2023-07-23).

3 Fletcher https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed#ft1.

4 Smith "15% of American Adults Have Used Online Dating Sites or Mobile Dating Apps" (11 February 2016) https://www.pewresearch.org/internet/2016/02/11/15-percent-of-american-adults-have-used-online-dating-sites-or-mobile-dating-apps/ (accessed 2023-07-23); Lauckner, Truszczynski, Lambert, Kottamasu, Meherally, Schipani-McLaughlin, Taylor and Hansen "'Catfishing', Cyberbullying, and Coercion: An Exploration of the Risks Associated with Dating App Use Among Rural Sexual Minority Males" 2019 23(3) *Journal of Gay & Lesbian Mental Health* 289 289.

5 See Watney "Cybercrime" in Papadopoulos and Snail (eds) *Cyber@Law: The Law of the Internet in South Africa* 4ed (2022) 463.

6 It was reported in 2021 that South Africa had the third most cybercrime victims worldwide, and that they suffered an estimated loss of R2.2 billion per year; see Interpol *African Cyberthreat Assessment Report: Interpol's Key Insight into Cybercrime in Africa* (2021) 9; Accenture "Insight into the Cyberthreat Landscape in South Africa" 2020 https://www.accenture.com/acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf#zoom=50 (accessed 2023-07-23).

7 See foreword of SADC *SADC Model Law on Computer Crime and Cybercrime* (2013); see also Van der Linde "Electronic Offences" in *South African Criminal Law and Procedure Volume III: Statutory Offences* RS 32 (2022) G8–2.

8 African Union *African Union Convention on Cyber Security and Personal Data* Protection (2014). Adopted: 27/06/2014; EIF: 08/06/2023.

9 See Preamble, as well as art 28, of the AU Convention.

10 (2001) ETS 185. Adopted: 23/11/2001; EIF: 1/07/2004.

11 See Ch III of the Budapest Convention.

12 See art 12 of the Model Law; art 30(1)(a) and (b) of the AU Convention and art 8 of the Budapest Convention. South Africa is a signatory to the AU Convention (which came into force on the 8th of June 2023) but has not ratified it – see African Union "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf) (accessed 2024-06-04). South Africa is not bound by the SADC Model Law as it is merely a model law and has neither signed nor acceded to the Budapest Convention.

The South African Cybercrimes Act[13] (Cybercrimes Act) came into force on 1 December 2021. The aims of this Act (according to the Preamble) include the creation of cybercrime-related offences, the criminalisation of the disclosure of harmful data messages, and the regulation of procedural matters such as jurisdiction and mutual assistance. Section 8 of the Cybercrimes Act specifically criminalises cyber fraud. However, this new statutory offence does not repeal, replace or amend the common-law crime of fraud.

The aim of this contribution is threefold: first, it defines and explains the phenomena of online dating fraud and "catfishing"; secondly, it analyses the offence of cyber fraud and common-law fraud to evaluate whether, how and to what extent this conduct fits into the proscriptive ambit of these offences; thirdly, this contribution considers procedural matters such as the splitting of charges and the duplication of convictions, as well as competent verdicts and the sentencing of online romance fraudsters.

2 DEFINING ONLINE DATING FRAUD AND CATFISHING[14]

Online dating fraud or scams may take many forms. Scammers however most often misrepresent their intentions in entering a romantic relationship with their intended victim or target in order to defraud them.[15] Victims are often lured in through dating websites and mobile dating applications such as Tinder,[16] Grindr, Hinge and Bumble. Scams may also occur on social media websites such as Facebook and Instagram, and on messaging applications such as WhatsApp, or even via email.[17] Scammers groom potential victims over time to obtain their trust.[18] In order to foster a sense of trust, fraudsters regularly take on the personas (whether based on real persons or fabricated) of people in trusted professions or positions of

13 19 of 2020.

14 In this article, online dating fraud and catfishing are discussed together as the two concepts often overlap.

15 Whitty "The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam Get Access Arrow" 2013 53(4) *British Journal of Criminology* 665 666.

16 See Staff Writer "Beware These Dating Scams Targeting South Africans This Valentine's Day – Even on Tinder" (14 February 2023) https://businesstech.co.za/news/lifestyle/664195/beware-these-dating-scams-targeting-south-africans-this-valentines-day-even-on-tinder/ (accessed 2023-07-23); Anonymous "Online Dating Scams and How to Avoid Them" (undated) https://www.kaspersky.com/resource-center/threats/beware-online-dating-scams (accessed 2023-07-23). The Tinder terms of use also explicitly prohibit its users from "[s]olicit[ing] money or other items of value from another user, whether as a gift, loan, or form of compensation" – see Tinder "Tinder Terms of Use" (2024) https://policies.tinder.com/terms/us/en/ (accessed 2024-04-19).

17 Eseadi, Ogbonna, Otu and Ede "Hello Pretty, Hello Handsome!: Exploring the Menace of Online Dating and Romance Scam in Africa" in Chan and Adjorlolo (eds) *Crime, Mental Health and the Criminal Justice System in Africa* (2021) 66.

18 Anonymous https://www.kaspersky.com/resource-center/threats/beware-online-dating-scams; Whitty "Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims" 2020 26 *European Journal on Criminal Policy and Research* 399 402.

authority, such as military personnel or aid workers.[19] The communication between the victim and the scammer is "frequent and intense" to hasten the grooming process.[20] These perfidious lovers often declare their love or feelings relatively early in the romance to manipulate their victims.[21] Unfortunately, their romantic promises and declarations of love are only fantasies sketched to lure their potential victims as the scammer intends eventually to defraud the victim.

The scammer initially asks for an insignificant amount of money or small gifts but these requests significantly increase in value as the "relationship" develops.[22] Often, the scammer develops a "personal emergency" that suddenly necessitates the need for sums of money, often in the form of a loan.[23] This may include paying legal fees, aeroplane tickets and hospital bills.[24] A good example is the so-called "Tinder Swindler", Simon Hayut, who went by the pseudonym Simon Leviev, and pretended to be the son of diamond magnate Lev Leviev.[25] He would seduce women on Tinder and assert (mainly on WhatsApp) that his enemies were after him, requiring him to go into hiding. He would then claim that he could not access his bank accounts and ask the women to advance him a sum of money that he promised to repay.[26] As he had (mis)represented himself as the son of a mogul, the victims had no issue in providing him with the money. He, however, went out of his way to evade repayment.[27]

A South African victim alleged that her so-called boyfriend had requested money from her but promised to repay her as soon as he received monies owed to him.[28] The alleged fraudster employed emotional blackmail techniques when she refused to transfer the funds, asserting that she did not love him, despite his being willing to marry her and purchase a house for her.[29] She alleges that she was defrauded of R500 000 over a period of nine months, leaving her penniless.[30] It later emerged that her online partner was not the person depicted in the images he shared with her and was

---

19 Eseadi *et al* in Chan and Adjorlolo (eds) *Criminal Justice* 66; Koon and Yoong "Preying on Lonely Hearts: A Systematic Deconstruction of an Internet Romance Scammer's Online Lover Persona" 2013 23(1) *Journal of Modern Languages* 28 30.

20 Whitty and Buchanan "The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial" 2016 16(2) *Criminology & Criminal Justice* 176 177.

21 *Ibid*.

22 Whitty 2013 *British Journal of Criminology* 666; Whitty and Buchanan 2016 *Criminology & Criminal Justice* 177; Eseadi *et al* in Chan and Adjorlolo (eds) *Criminal Justice* 67.

23 Eseadi *et al* in Chan and Adjorlolo (eds) *Criminal Justice* 67.

24 Whitty 2020 *European Journal on Criminal Policy and Research* 403.

25 DiLillo "Who Is the Tinder Swindler?" (14 February 2022) https://www.netflix.com/tudum/articles/who-is-tinder-swindler-real-shimon-hayut (accessed 2023-07-23).

26 *Ibid*.

27 *Ibid*.

28 Carte Blanche "Online Love Scams" (13 February 2020) https://youtu.be/Rl3FLdxjgO0 (accessed 2023-07-23).

29 *Ibid*.

30 *Ibid*.

contracted by a syndicate to scam her.[31] It is not uncommon for romance scammers to operate in vast fraud networks or organised syndicates.[32]

Victims of online dating fraud or scams appear to be predominantly women over 50.[33] Over and above the monetary losses that victims may suffer, they also suffer a broad spectrum of emotional harm such as self-doubt, shock, a loss of social status, embarrassment, anxiety and stress, and the ordeal can also lead to post-traumatic stress disorder.[34] Victims also feel ostracised by colleagues, friends and family.[35] They are often doubly traumatised owing to the loss not only of the scammed funds but also the (sham) relationship.[36] Interestingly, a study conducted in 2016 showed that participants experienced more trauma from the dissolution of the relationship than the (often substantial) loss of money.[37]

A romance scam ends only when the victim discovers the true intentions of the scammer and discontinues their financial support of the scammer,[38] or when the scammer reaches a predetermined financial goal.[39]

As mentioned above, the South African victim was scammed by someone who misrepresented himself by using images of another person. This is known as "catfishing". This term was popularised by the documentarian Nev Schulman, following his own catfishing experience.[40] It turned out that not only was the woman depicted in the images shared by his online paramour not her, but she was also married.[41] She used publicly available images of a model who, of course, did not know or authorise the use of her likeness.[42] The phrase originates from the husband of the fraudster, Angela Wesselman-Pierce, who recounted how cod fishermen would add catfish to their cod hauls to keep the "cod active and alert until arrival". The implication

---

31 *Ibid*.

32 Rege "What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud" 2009 3(2) *International Journal of Cyber Criminology* 494 501–502; Whitty and Buchanan 2016 *Criminology & Criminal Justice* 177. See also *Otubu v Director of Public Prosecutions, Western Cape* 2022 (2) SACR 311 (WCC) par 7, where the bail applicants in that case were wanted in the United States for online romance scams. The appellant was part of a syndicate known as the Black Axe.

33 Peachey "Women 'Victims in 63% of Romance Scams'" (10 February 2019) https://www.bbc.com/news/business-47176539 (accessed 2023-07-23); Carte Blanche https://youtube/Rl3FLdxjgO0.

34 Whitty and Buchanan 2016 *Criminology & Criminal Justice* 178 180; Lauckner *et al* 2019 *Journal of Gay & Lesbian Mental Health* 291.

35 Whitty and Buchanan 2016 *Criminology & Criminal Justice* 181; Carte Blanche https://youtu.be/Rl3FLdxjgO0.

36 Whitty and Buchanan 2016 *Criminology & Criminal Justice* 182.

37 Whitty and Buchanan 2016 *Criminology & Criminal Justice* 189–190.

38 Whitty 2013 *British Journal of Criminology* 666.

39 Rege 2009 *International Journal of Cyber Criminology* 502.

40 See IMDb "Catfish" (2010) https://www.imdb.com/title/tt1584016/ (accessed 2023-07-23).

41 Kaufman "The Woman Behind 'Catfish's' Mystery" (5 October 2010) https://www.latimes.com/archives/la-xpm-2010-oct-05-la-et-catfish-lady-20101005-story.html (accessed 2023-07-23).

42 Santi "'Catfishing': A Comparative Analysis of U.S. v. Canadian Catfishing Laws & Their Limitations" 2019 44 *Southern Illinois University Law Journal* 75 76. Also see Ndyulo "Protecting the Right to Identity Against Catfishing: What's the Catch?" 2023 44 *Obiter* 308 308–330.

is that catfish, such as his wife, keep the lives of others exciting.[43] This (perhaps distasteful) metaphor has now evolved to be understood as denoting "a person who sets up a false personal profile on a social networking site for fraudulent or deceptive purposes".[44] The catfish uses the images of third parties to trick the target into believing that they (the catfish) are the persons depicted in the images.[45] The catfish usually selects images of attractive people, including models and athletes.[46] Catfish often create elaborate online identities in order to manipulate their targets into entering into relationships with them.[47] Catfishing and online dating scams often also overlap, as romance fraudsters are most likely to use fake profiles (in other words, not their own photos or social media accounts) to seduce their victims.[48] The profiles are typically accompanied by flattering text descriptions of their personality, including their personal interests, life story, and values.[49] However, not all catfish are romance scammers, as their motivations for employing false profiles may be unrelated to any financial gain. Some people may use a catfish persona owing to loneliness, and believe that using a more attractive persona may make them more popular, while others are dissatisfied with their physical appearance and struggle with their self-esteem.[50] Others have also used it as a way to freely explore their sexuality and gender identity.[51]

With the recent rise in lifelike images generated by artificial intelligence (AI), also known as "deepfakes",[52] there is now even less need to appropriate *existing* images to create (fake) online personas. AI is employed "to produce new identities and duplicate existing ones, to create a video, sound recording, or photograph of a scene that did not take place".[53] Not only can images or videos be created out of whole cloth, but the likeness of real persons can be superimposed onto the body of another.[54]

---

43 Merriam-Webster "Catfish" (undated) https://www.merriam-webster.com/dictionary/catfish (accessed 2023-07-23).

44 Merriam-Webster https://www.merriam-webster.com/dictionary/catfish. Also see Cambridge Dictionary "Catfish" (undated) https://dictionary.cambridge.org/dictionary/english/catfish (accessed 2023-07-23).

45 Whitty 2013 *British Journal of Criminology* 666.

46 Coluccia, Pozza, Ferretti, Carabellese, Masti and Gualtieri "Online Romance Scams: Relational Dynamics and Psychological Characteristics of the Victims and Scammers. A Scoping Review" 2020 16 *Clinical Practice & Epidemiology in Mental Health* 24 25; Smith, Smith and Blazka "Follow Me, What's the Harm: Considerations of Catfishing and Utilizing Fake Online Personas on Social Media" 2017 27 *Journal of Legal Aspects Sport* 32 35–36.

47 Cohen "Angling for Justice: Using Federal Law to Reel in Catfishing" 2019 2 *The Journal of Law and Technology at Texas* 51 54.

48 Carte Blanche https://youtu.be/Rl3FLdxjgO0.

49 Coluccia *et al* 2020 *Clinical Practice & Epidemiology in Mental Health* 25.

50 Santi 2019 *Southern Illinois University Law Journal* 81–82.

51 Santi 2019 *Southern Illinois University Law Journal* 82.

52 Deepfake is a portmanteau word consisting of "deep learning" and fake. Deep learning, according to Mashinini, is a process which "enables computers to learn independently how to perform human tasks, using increased computing power"; see Mashinini "The Impact of Deepfakes on the Right to Identity: A South African Perspective" 2020 32(3) *SA Merc LJ* 407 408–409.

53 Mashinini 2020 *SA Merc LJ* 408.

54 Mashinini 2020 *SA Merc LJ* 411.

In light of the above, the next section sets out the offence of fraud, both under the common law and the Cybercrimes Act, to evaluate whether and to what extent online dating fraud and/or catfishing fall under the scope of the offence.

3 BROAD OVERVIEW OF THE CRIME OF FRAUD

Fraud is criminalised both under the common law and the Cybercrimes Act. The elements of the common-law crime require there to be a misrepresentation, prejudice (or even potential prejudice), as well as unlawfulness and intent.[55] Section 8 of the Cybercrimes Act reads as follows:

> "Any person who unlawfully and with the intention to defraud makes a misrepresentation
> (*a*) by means of data or a computer program; or
> (*b*) through any interference with data or a computer program as contemplated in section 5(2) (*a*), (*b*) or (*e*) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(*a*),
> which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud."

The terms "data", "computer program", "computer data storage medium" and "computer system" are all defined under Chapter 1 of the Cybercrimes Act. "Data" means "electronic representations of information in any form", while "computer program" means "data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function". "Computer data storage medium", in turn, means:

> "any device from which data or a computer program is capable of being reproduced or on which data or a computer program is capable of being stored, by a computer system, irrespective of whether the device is physically attached to or connected with a computer system."

A "computer system" means

> "(*a*) one computer; or
> (*b*) two or more interconnected or related computers, which allow these interconnected or related computers to
> (i) exchange data or any other function with each other; or
> (ii) exchange data or any other function with another computer or a computer system."

The offence under the Cybercrimes Act is therefore "virtually identical" to the common-law offence of fraud.[56] The only substantive difference is that the offence of cyber fraud requires the accused to have committed the crime through specific means, namely "by means of data or a computer program […] or through any interference with data or a computer program".

---

[55] Hoctor *Snyman's Criminal Law* 7ed (2020) 461.

[56] Van der Linde *Criminal Law and Procedure* G8–11.

4 CONSIDERING ONLINE ROMANCE FRAUD AND CATFISHING AS INSTANCES OF THE COMMON-LAW CRIME OF CYBER FRAUD

As the common-law crime of fraud and cyber fraud are "virtually identical" save for the fact that the latter must be committed through specific means (and carry certain prescribed sentences), the ensuing section discusses the elements of the two crimes simultaneously. Where any substantive differences exist, such differences are highlighted.

4 1 Misrepresentation

The *actus reus* of both crimes is a misrepresentation. This misrepresentation must amount to a "perversion or distortion of the truth".[57] Fraud can occur broadly through spoken or written words or by conduct and may be explicit or implied.[58] There are two sets of misrepresentation that occur during the course of a dating scam. First, an online dating scammer distorts the truth by misrepresenting their feelings for the victim, when the victim is merely a target for financial gain. The second, interrelated misrepresentation concerns the scammer's intention to pay back the money or "make good" with the victim during the relationship. These representations are the ones that will form the core of the fraud investigation and prosecution. As outlined above, fraudsters often create false emergencies to create a sense of urgency to manipulate their target further. This usually goes hand in hand with an undertaking to repay (or make good with) the victim at a later stage.

Under the Cybercrimes Act, the misrepresentation may only take place by means of data or a computer program, or through interference with data or a computer program, or interference with a computer data storage medium or a computer storage system. As "data" is defined as "electronic representations of information in any form", messages sent via either the Internet or any type of mobile application such as Tinder will certainly fall within the ambit of the offence under section 8 of the Cybercrimes Act.

4 2 Prejudice

The misrepresentation must cause actual or potential prejudice to the victim. It is, therefore, not necessary for the harm actually to manifest. Consequently, it is not required to prove that the victim was in fact misled by the misrepresentations.[59] Hoctor describes the term "potential prejudice" as one with multiple possible meanings. It may denote, objectively viewed, at least a risk of prejudice or even the likelihood thereof.[60] This objective view

---

57 Hoctor *Snyman's Criminal Law* 462; Milton *South African Criminal Law and Procedure Volume II: Common-Law Crimes* 3ed (1996) 705.

58 Burchell *Principles of Criminal Law* 5ed (2016) 745–746; Hoctor *Snyman's Criminal Law* 462.

59 Hoctor *Snyman's Criminal Law* 466.

60 *Ibid*.

or test also means that the potential prejudice must be reasonable and not too remote.[61] A likelihood of prejudice does not denote a probability that the prejudice will occur but rather only a possibility.[62] Furthermore, it is irrelevant if the target of the fraud knew that assertions made by the accused were false.[63]

The scam may unravel for a multitude of reasons. This may include the victim not being able to find the resources to pay the scammer, or the victim (or someone else) discovering the true intentions of the scammer.[64] Even if a scam unravels before it runs its course, the prejudice element of the crime will be met if the State establishes that there was potential prejudice.

Under the common law, the prejudice may be proprietary or non-proprietary.[65] There is no reference to the type of proprietary prejudice required under section 8 of the Cybercrimes Act. There is also no reason to believe that this form of prejudice has been codified into the Cybercrimes Act, as the legislature has been clear that both actual and potential harm are proscribed, although it is silent on the type of proprietary prejudice. Two regional instruments, however, are clear on the matter. Article 12 of the SADC Model Law is quite prescriptive; it specifically requires that there be "a loss of property" for the victim, and an "economic benefit" for the culprit,[66] while article 8 of the Budapest Convention similarly requires "an economic benefit" for the culprit. Neither of these instruments binds South African courts, but courts may consider them to cure any uncertainty regarding non-proprietary prejudice.

The potential exclusion of non-proprietary prejudice under section 8 of the Cybercrimes Act does not detract from the fact that instances of online dating fraud invariably involve a financial objective by the fraudster.

4 3 Intent

Fraud is committed with the intention of defrauding the victim, and the accused must be aware that their representations are false.[67] In such an instance, the fraud would be committed with intent, specifically *dolus directus*. However, *dolus eventualis* will also satisfy the intent requirement, as it is sufficient for the State to prove that the accused foresaw the possibility that their representations may be false, but recklessly went on to make them nevertheless.[68] Online romance scammers are likely to commit

61 *Ibid*.
62 *Ibid*.
63 Kemp (ed) *Criminal Law in South Africa* 4ed (2023) 471; Hoctor *Snyman's Criminal Law* 465.
64 Whitty and Buchanan 2016 *Criminology & Criminal Justice* 179.
65 Hoctor *Snyman's Criminal Law* 466; Burchell *Principles* 749–750.
66 Neither of these terms is defined under the Model Law; they should be given their ordinary meanings.
67 Kemp (ed) *Criminal Law* 470; Hoctor *Snyman's Criminal Law* 467.
68 *Ex Parte Lebowa Development Corporation Ltd* [1989] 4 All SA 492 (T); Kemp (ed) *Criminal Law* 470; Hoctor *Snyman's Criminal Law* 467.

fraud or cyber fraud with *dolus directus* as they intend from the outset to defraud the victim.

4 4 Unlawfulness

If there is no ground of justification to excuse the conduct of the accused, the misrepresentations will be considered unlawful. However, coercion or compulsion[69] or obedience to superior orders may exclude the element of unlawfulness.[70] Burchell asserts that false declarations of love to obtain "sexual favours" fall under a type of conduct where there has been "tacit acceptance" and will not be subject to prosecution.[71] False declarations of love are at the heart of romance scams, but the prejudice may be differentiated from Burchell's assertion. The benefit sought by a romance scammer is proprietary, while the benefit in Burchell's example is sexual. Romance scammers, in fact, rarely meet their victims. A notable exception is the Tinder Swindler, Simon Hayut.

4 5 Causation

It has been submitted that causation is a superfluous element of the common-law crime of fraud. Burchell and Kemp do not even discuss it as an element of the crime. Hoctor agrees that the element is superfluous, as prejudice has received such a broad interpretation by the courts that it has been rendered meaningless and superfluous.[72] Milton asserted that it was "logically redundant" to require causation in cases involving potential fraud.[73]

Section 8 of the Cybercrimes Act states that the accused must make "a misrepresentation … which causes actual or potential prejudice to another person". It is submitted that courts are unlikely to require the State to prove causation; although the definitions of the common-law crime of fraud, stated by the three authors above, all still employ the word "causes",[74] they nevertheless regard it as superfluous or do not discuss it all.

It would, in any event, usually be simple for the prosecution to prove, under section 8 of the Cybercrimes Act, that the misrepresentations by the scammer led to financial prejudice.

4 6 Evaluation

It is clear that the characteristics of an online dating scam fall within the ambit of either the common-law crime of fraud, or the cyber fraud offence under the Cybercrimes Act. Two (albeit minute) questions remain: whether the Cybercrimes Act covers non-proprietary prejudice; and whether

---

69 Kemp (ed) *Criminal Law* 470; Hoctor *Snyman's Criminal Law* 467.
70 Hoctor *Snyman's Criminal Law* 467.
71 Burchell *Principles* 745.
72 Hoctor *Snyman's* Criminal Law 467.
73 Milton *Criminal Law* 719.
74 Burchell *Principles* 742; Hoctor *Snyman's Criminal Law* 461; Kemp (ed) *Criminal Law* 468.

causation is an essential element under the same. It is submitted that the answer to both of these questions is probably "no".

5 PROCEDURAL MATTERS

5 1 Splitting of charges and duplication of convictions

As *dominus litus*, the State may charge the accused with all offences arising from a specific factual matrix.[75] This is known as the splitting of charges and is a permissible prosecutorial practice under the Criminal Procedure Act[76] (CPA). This, however, does not entitle the court to convict an accused of all charges against them.[77] The duplication of convictions is unlawful. In *S v Whitehead*,[78] Combrinck JA held that "it is a fundamental principle of our law that an accused should not be convicted and sentenced in respect of two crimes when he or she has committed only one offence", and this protection is enshrined under section 35(3) of the Constitution.[79] An accused may therefore be charged with common-law fraud and cyber fraud in the same charge sheet or indictment, in the alternative, but a court is unlikely to convict an accused of both offences.

Courts have developed two broad tests to determine when a conviction on two separate charges constitutes an unlawful duplication of convictions. The "evidence test" requires a court to consider whether the evidence required to prove one offence also proves another.[80] The "intent test" evaluates whether a series of criminal actions are carried out with a single intent.[81] It would constitute an unlawful duplication of convictions where an accused is charged with committing various acts arising from a "continuous criminal transaction".[82] These tests are nevertheless not decisive or exhaustive and must always be considered with a healthy dose of common sense.[83] As the common-law and statutory offences are "virtually identical" save for the latter requiring that the crime be committed in a specific manner, a conviction on both offences is likely to constitute an impermissible duplication of offences.

However, it is cognisable that a certain series of interactions could give rise to a set of charges under the Cybercrimes Act and the common law. This is particularly where the representations were made both online as well as in person. Whether a prosecutor would laboriously charge and prosecute

---

75 S 83 of the CPA.

76 51 of 1977.

77 S 336 of the CPA

78 2008 (1) SACR 431 (SCA).

79 The Constitution of the Republic of South Africa, 1996. See also, *S v Whitehead* supra par 10.

80 *S v Whitehead supra* 39.

81 *S v Whitehead supra* par 42

82 *S v Davids* 1998 (2) SACR 313 (C) 316; Van der Linde "Managing and Participating in a Criminal Enterprise Under POCA: Duplication of Convictions? A Discussion of the Conflict Between *S v Prinsloo* and *S v Tiry*" 2022 139(3) *South African Law Journal* 526 530.

83 *S v Grobler* 1966 (1) SA 501 (A) 523; *Whitehead supra* par 35.

someone under the common law and the Cybercrimes Act is dubious, especially because the broadly defined offence under the common law is wide enough to encompass all instances of the offence under the Cybercrimes Act. However, there are certain procedural advantages to prosecuting someone under the Cybercrimes Act, as minimum sentences would apply in certain scenarios. These scenarios are canvassed below. The most apposite route to follow is charging an accused under the Cybercrimes Act, and charging them with common-law fraud in the alternative. If a prosecutor fails to do so, a court will also be able to convict the accused of a myriad other offences owing to the operation of competent verdicts.

5 2 Competent verdicts

Where the State fails to prove an offence beyond reasonable doubt, and yet, on the evidence, establishes a (usually lesser) offence with which the accused was not charged, a court may convict the accused of the offence where such an offence is a competent verdict to the charged offence.[84] The offence now established on the facts must not have been either a charge or an alternative charge in the charge sheet or indictment.[85] Competent verdicts are only permissible if authorised by statute,[86] and are contained mainly under Chapter 26 of the CPA. There are two broad provisions relating to attempt[87] and accessories after the fact[88] that enable courts to convict accused persons of these offences if established by the evidence, and where the prosecution has failed to prove the substantive offence beyond a reasonable doubt. Chapter 26 also contains a range of specific offences on which courts are empowered to impose competent verdicts, including convicting someone of culpable homicide instead of murder or attempted murder.[89] Offences not explicitly mentioned in Chapter 26 of the CPA may still be considered competent verdicts under section 270 if another offence containing "the essential elements of that offence is included in the offence so charged". As there are no competent verdicts listed for the common-law crime of fraud under Chapter 26 of the CPA, could section 270 of the CPA be invoked to convict an accused of the crime of cyber fraud?[90] The statutory offence requires cyber fraud to be committed through specific means, including "by means of data or a computer program" or through "interference with data or a computer program". Unless the instance of common-law fraud was already "cyber" in nature, it is unlikely that these essential elements would have formed part of the common-law charge. In such an event, it may have been more appropriate to charge the accused with cyber fraud in the first place.

---

84 Joubert (ed) *Criminal Procedure Handbook* 13ed (2020) 389.

85 As envisaged under s 83 of the CPA; see Joubert *Handbook* 389.

86 Theophilopoulos (ed) *Criminal Procedure in South Africa* (2020) 350; Joubert *Handbook* 389.

87 S 256 of the CPA.

88 S 257 of the CPA.

89 S 258 of the CPA.

90 See Van der Merwe "Competent Verdict" in Du Toit and Van der Merwe *Commentary on the Criminal Procedure Act* vol 3 (RS 68, 2022) 26–26.

The Cybercrimes Act also contains a comprehensive list of competent verdicts under section 18 of the Act. The unlawful interception of data,[91] unlawfully accessing data,[92] using or possessing hardware or software tools for specific purposes,[93] and acquiring or possessing a password, access code or similar device or data to commit cyber fraud[94] or cyber extortion[95] are competent verdicts on a charge of cyber fraud. An accused may also be convicted of the common-law crime of fraud or attempted fraud,[96] common-law forgery, uttering or an attempt to commit those crimes,[97] or common-law theft or attempted theft.[98]

A court may also convict an accused of an attempt[99] or conspiracy[100] to commit cyber fraud. An accused may also be convicted of aiding, abetting, inducing, inciting, instigating, instructing, commanding or procuring another person to commit cyber fraud.[101] Such an accused will be liable to receive the same punishment as applies to the substantive offence.[102] It is usual practice not to subject the accused to the same punishment for incitement or conspiracy as for committing the substantive offence.[103]

Where the State charges an accused only with the statutory offence under section 8, and does not charge them with common-law fraud in the alternative, such an accused may be convicted of common-law fraud as the aforementioned offence is a competent verdict to cyber fraud. A scenario where an accused is charged with common-law fraud, but is not convicted, and yet is found guilty of cyber fraud in terms of section 270 of the CPA is unlikely.

5 3 Sentencing

The Cybercrimes Act does not prescribe a sentence for “ordinary” instances of cyber fraud that do not fall within the ambit of the minimum sentences. A court is then required to impose a sentence as envisaged under section 276

91 S 18(6)(*a*), read with s 2(1) of the Cybercrimes Act.
92 S 18(6)(*a*), read with s 2(2) of the Cybercrimes Act.
93 S 18(6)(*b*), read with ss 4(1), 5(1) and 6(1) of the Cybercrimes Act.
94 S 18(6)(*c*), read with ss 7(1), 7(2) and 8 of the Cybercrimes Act.
95 S 18(6)(*d*), read with s 9(1) and (2) of the Cybercrimes Act.
96 S 18(6)(*e*) of the Cybercrimes Act.
97 S 18(6)(*f*) of the Cybercrimes Act.
98 S 18(6)(*g*) of the Cybercrimes Act.
99 S 17(*a*) of the Cybercrimes Act.
100 S 17(*b*) of the Cybercrimes Act.
101 S 17(*c*) of the Cybercrimes Act.
102 S 17 of the Cybercrimes Act.
103 Burchell *Principles* 539; Hoctor *Snyman's Criminal Law* 263. This was also confirmed by the Constitutional Court in *Economic Freedom Fighters v Minister of Justice and Correctional Services* 2021 (2) SA 1 (CC) (*EFF*), as judicial officers still maintain their discretion to impose the most appropriate sentence in the circumstances; see *EFF supra* par 27, citing *S v Toms; S v Bruce* 1990 (2) SA 802 (A) 813. Courts also retain their ordinary sentencing discretion whereby the offence, offender and the interests of society are considered when considering an appropriate sentence; see *S v Zinn* 1969 (2) SA 537 (A) 540.

of the CPA.[104] The minimum sentences under the Cybercrimes Act would apply where cyber fraud was committed by the accused or "with the collusion or assistance" of another, and that person or persons

> "who as part of their duties, functions or lawful authority were in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system belonging to another person in respect of which the offence in question was committed."[105]

If the cyber fraud has been committed under those circumstances, a court must impose a sentence of direct imprisonment "unless substantial and compelling circumstances justify" imposing a sentence other than direct imprisonment (with or without a fine).[106] This sentence may also not be suspended.[107]

The Criminal Law Amendment Act[108] (CLAA) also creates certain minimum sentences for cyber fraud.[109] Instances where minimum sentences fall into four broad categories relating to the status of the offender:

1. The fraudulent acts involved amounts exceeding R500 000.
2. The defrauded amount exceeded R100 000 *and* the offence was committed in furtherance or execution "of a common purpose or conspiracy".[110]
3. The fraudulent acts exceeded R100 000 *and* the offence was committed under certain specific circumstances. This is where someone acts alone, receives assistance or colludes with others. Secondly, the accused must have "as part of his or her duties, functions or lawful authority [been] in charge of, in control of, or had access to data, a computer program, a computer data storage medium or a computer system of another person".

---

104 S 19(4) of the Cybercrimes Act. S 276 of the CPA applies if a sentence is not prescribed in terms of other legislation. S 276(1) reads as follows:

> "Subject to the provisions of this Act and any other law and of the common law, the following sentences may be passed upon a person convicted of an offence, namely
>
> (*a*) .....
>
> (*b*) imprisonment, including imprisonment for life or imprisonment for an indefinite period as referred to in section 286B (1);
>
> (*c*) periodical imprisonment;
>
> (*d*) declaration as an habitual criminal;
>
> (*e*) committal to any institution established by law;
>
> (*f*) a fine;
>
> (*h*) correctional supervision;
>
> (*i*) imprisonment from which such a person may be placed under correctional supervision in the discretion of the Commissioner or a parole board."

105 S 16(6) of the Cybercrimes Act.

106 S 16(6)(*a*) of the Cybercrimes Act.

107 S 16(6)(*b*) of the Cybercrimes Act, read with s 297(4) of the CPA. The latter provision permits a court to suspend any prescribed minimum punishment for periods not exceeding five years and impose any condition as described under s 297(1)(*a*)(i) of the CPA.

108 105 of 1997.

109 Under s 51(2)(a)(*i*), read with Part II of Schedule 2 of the CLAA.

110 Part II of Schedule 2 of the CLAA.

4. The last category involves fraudulent acts by law enforcement officers.[111] They fall within the ambit of the provisions if the fraudulent act or acts relate to amounts exceeding R10 000 or, while a police officer, they acted in concert with others as described in 2 or was in charge of the systems listed in 3.

First-time offenders under any of these categories will face imprisonment of at least 15 years,[112] while second-time offenders will face a minimum of 20 years.[113] Persons who are third-time (and subsequent) offenders face a minimum of 25 years' imprisonment.[114] Just as with the prescribed sentences under the Cybercrimes Act, a court may only deviate from the imposition of the minimum sentence if "substantial and compelling circumstances exist" to justify imposing a lesser sentence.[115]

The threshold for the applicability of the minimum sentence regime is much lower for law enforcement officers. This is so because a single act of cyber fraud by a law enforcement officer involving an amount of R10 000 would invoke the provisions, as opposed to amounts of R100 000 and R500 000 respectively when persons who are not law enforcement officers are involved.

The minimum sentences appear harsher than courts would impose for common-law fraud and, reviewing a number of cases, sentences rarely involved a term of imprisonment of 15 years[116] or more.[117]

6 CONCLUSION

Online fraud, especially online romance fraud, is becoming an increasingly serious threat. Clearly, the common-law crime of fraud, as well as the

111 The term "law enforcement officer" is described under the CLAA as including members of the National Intelligence Agency or the South African Secret Service (under s 3 of the Intelligence Services Act 65 of 2002) and correctional officials working for the Department of Correctional Services or authorised persons in terms of the Correctional Services Act 111 of 1998.

112 S 51(2)(i) read with Part II of Schedule 2 of the CLAA.

113 S 51(2)(ii) read with Part II of Schedule 2 of the CLAA.

114 S 51(2)(iii) read with Part II of Schedule 2 of the CLAA.

115 S 51(3)(*a*) of the CLAA. A comprehensive discussion of "substantial and compelling circumstances" falls beyond the scope of this contribution. The *locus classicus* regarding the imposition of minimum sentences under the CLAA, an deviations therefrom, is *S v Malgas* 2001 (1) SACR 469 (SCA). The Supreme Court of Appeal (SCA) there set out a step-by-step approach as to the deviation from the minimum sentence and the meaning of "substantial and compelling circumstances". The Constitutional Court in *S v Dodo* 2001 (3) SA 382 (CC) later affirmed this approach. There is no reason to believe that the term "substantial and compelling circumstances" under the Cybercrimes Act should be ascribed a different meaning from that under the CLAA. Therefore, it is submitted that CLAA jurisprudence on the matter may be transposed to matters under the Cybercrimes Act.

116 See *S v Rautenbach* 2015 JDR 0228 (GP) (involving fraud of R1 339 560), *S v Boshoff* 2013 JDR 2181 (ECG) (involving fraud of R35 000) and *S v Ntozini* 2020 JDR 1983 (ECG) (involving fraud of R19 722 000 and the hacking of the Nelson Mandela Metropolitan Municipality by a syndicate).

117 See *S v Hattingh* 2014 JDR 0491 (FB), where the accused was sentenced to 20 years' imprisonment (involving fraud of R52 000 000).

offence under section 8 of the Cybercrimes Act, adequately proscribes the typical *modus operandi* of a romance scammer. A prosecutor is entitled to charge a suspect with either of these offences, or charge them in the alternative. The decision on how to formulate the charges will depend on a constellation of considerations, but sentencing is a significant one, as the accused will face minimum sentences under a set of circumstances described under the CLAA. Courts are unlikely to be entitled to convict an accused of both offences, as that would constitute an unlawful duplication of offences owing to the substantive similarity of the two offences. In any event, a court is entitled to convict an accused of common-law fraud if *cyber* fraud is not proven, or even conspiracy, incitement, or aiding and abetting cyber fraud.

One can, however, question the existence of an independent offence of cyber fraud as it does not *add* to the scope of the common-law offence. In fact, it limits the scope of the offence. The true utility of the offence under section 8 is the fact that the accused faces harsher punishment. However, this could have been achieved through amendments to the CLAA. The minimum sentences are, in any case, contained under the CLAA. Nevertheless, if an independent offence serves the exclusive function of bringing attention to the proliferation of cyber fraud and the fact that it is a punishable offence, that is itself a commendable goal. This awareness is important not only for victims who might be unaware that romance scams are illegal but also for police officers who might consider such scams a mere risk of being an Internet user and not a crime.