The British Journal of Criminology, 2024, **XX**, 1–21
https://doi.org/10.1093/bjc/azae069
Original Manuscript

OXFORD

The Liminality of Fraud: Reimagining Fraud Theory to Inform Financial Crime Prevention

Nicola Harding, Emily Cooper, Tony Sales, Andy McDonald and Sarah Kingston*

*N. Harding, Department of Criminology, Lancaster University, Lancaster, UK; E. Cooper and S. Kingston, Department of Law and Policing, University of Central Lancashire (UCLAN), Preston, UK; email: ecooper2@uclan.ac.uk; T. Sales and A. McDonald, We Fight Fraud, London, UK

Utilizing knowledge from academics, practitioners and subject matter experts with lived experience of fraud, this paper offers four significant contributions to fraud theory. Firstly, we argue that fraudsters seek out liminal spaces. Secondly, the paper identifies that fraudsters do not always seek immediate financial gain. Thirdly, we argue that within liminal space, individuals are transformed into fraud victims or potentially 'co-offenders' used to target businesses. By understanding the importance of liminality for the success of fraudulent interactions, we propose that both on and offline spaces that are vulnerable to facilitating fraud can be identified. Finally, we make the argument that aspects of situational crime prevention can be utilized within liminal spaces at key points to prevent fraud.

KEY WORDS: fraud prevention, financial crime, liminality, liminal space, lived experience, situational crime prevention

INTRODUCTION

Fraud offences involve an element of dishonesty, as it is a social interaction that is based upon lying, deception and false pretences to gain a financial advantage (Fletcher 2007; Smith 2000). Fraud itself is not new, with reports dating back to 300BC when Hegestratos, a Greek sea merchant, took out a bottomry on his ship and cargo.[1] He planned to sell his goods and sink the ship, keeping the money, in a very early form of insurance fraud (Grabosky and Smith 1998; Adedoyin Isola *et al.* 2017). However, developments in technology, such as the creation of online spaces and the development of web 2.0, have changed the ways in which it is perpetrated globally (Yar 2013). As such, much contemporary fraud research has focussed upon 'cyber enabled' crimes

1 Bottomry is a maritime loan, where the shipowner borrows money and uses the ship or cargo as collateral (Trenerry 2009).

(Cross 2020). With many papers making distinctions between online/offline fraud, Cross (2020) asserts that the distinction is arbitrarily used in government policy, for funding, and by the media. The reality is that 'traditional communication methods, such as telephone, text messages and simple face-to-face communication, remain a vehicle for important elements of many fraud offences', including a combination of online and offline methods (Cross 2020: 112).

Due to the impact of fraud internationally upon businesses, the economy, broader criminal behaviour and the individual, fraud is examined by researchers across multiple disciplines. Some research has focussed upon specific types of fraud, such as insurance fraud (Warren and Schweitzer 2018), credit card fraud (Dal Pozzolo *et al.* 2014) romance fraud (Carter 2021), cryptocurrency fraud (Dutta *et al.* 2023) and sextortion (Cross *et al.* 2023), as well as fraud processes and parties involved, such as money laundering (Turner 2012; Levi 2020), money mules (Vedamanikam and Chethiyar 2020; Bekkers *et al.* 2023), the use of Artificial Intelligence (AI) for romance scams (Cross and Layt 2022; Fletcher *et al.* 2024) and prevention and detection (Aftabi *et al.* 2023). Other fraud research offers typologies of fraud (Button *et al.* 2009) or fraudsters (Kapardis and Krambia-Kapardis 2004), as well as the stages of fraud (Goffman 1952; Maurer 2000) and the fraud environment (Levi 1981; 2008). Theories of fraud have focussed on understanding the motivations of offenders (Cressey 1950; 1953; Ramamoorti 2008; Kranacher *et al.* 2010; Schuchter and Levi 2016; Vousinas 2019) the social interactions and environment in which fraud occurs (Levi 2008; Burgard and Schlembach 2013) and there has been a growing focus on victims of fraud (Button *et al.* 2014; Buchanan and Shutterstock 2019; Cross 2020). Yet, as Vousinas (2019) and Saluja *et al.* (2022) argue, following their reviews of fraud theory, this body of work needs to be updated to 'adjust to the current developments in the field and the growing fraud incidents' (Vousinas 2019: 375). Our unique contribution is to respond to this call to advance fraud theorization by co-producing fraud theory with experts by experience. It is rare that researchers work to understand the mechanics of various types of fraud directly with those who have first-hand experience of committing fraudulent activity and investigation in juxtaposition. Second, our novel contribution is to apply the lens of liminality to understand the fraudsters' actions and the fraud environment.

This paper is co-written with individuals with lived experience of committing fraud on an international scale, professional expertise in fraud prevention and detection in the United Kingdom and United States and researchers working in fraud and financial crime in the United Kingdom. We also consulted fraud and financial crime solutions providers who operate within the United Kingdom, Europe, Australia and New Zealand. Together we examine the mechanics of fraud from example case studies, romance fraud and invoice fraud, to develop a theoretical conceptualization of fraud and financial crime that focuses upon the physical and conceptual spaces within which fraud occurs. We propose that for fraud to occur, three forms of liminality need to be at play: liminal identity(ies), liminal space(s) and liminal context(s). Liminality is the concept of a threshold, it describes the state of being betwixt and between where an old world has been left behind, but we have not yet arrived at what is to come (Franks and Meteyard 2007). The fraudster utilizes the in-between-ness and ambiguity of the space to transform themselves, and their victim. Additionally, we re-frame fraud as being not necessarily an activity that seeks immediate financial advantage. Whilst financial gain will be the end goal, increasingly personal and company data, that can be used to commit further fraudulent and potentially more lucrative acts, often hold more value to some serious organized criminals than money alone. Because large sums of money are often more difficult to steal, personal data can enable a fraudster to steal money from the victim, and also take out loans in a target's name and purchase goods, thus increasing the 'fraud-target-reward ratio'. We also make the connection between fraud against the individual and fraudulent activity targeted at businesses, through the transformation of the individual fraud victim to accessory to commit fraud against an employer. If individuals and

organizations can recognize liminal spaces within their environment and activities and understand the way these spaces are vulnerable to criminals seeking to obtain money or personal data, then this theoretical concept can be used to inform the development of defences against fraud, financial and serious organized crime activities. Finally, this article moves from theory to practice, by utilizing the theoretical insights to develop situational crime prevention (SCP) techniques that could be employed to detect and prevent fraud.

THEORIZING FRAUD

The Fraud Triangle Theory (FTT) of Cressey (1950; 1953) and Fraud Diamond Theory (FDT) of Wolfe and Hermanson (2004) are the most significant attempts to explain the causes of fraud. Each of the models (FTT and FDT) identifies the key elements that lead perpetrators to commit fraud. Dorminey *et al.* (2010) describe how Cressey (1950; 1953) created the FTT after being influenced by the work of Edwin Sutherland (1940) and his development of the concept of white-collar crime. Cressey (1950; 1953) was interested in unethical and fraudulent behaviour when he developed the FTT. He said that for fraud to occur that there must be (1) perceived pressure, (2) opportunity and (3) rationalization.

Wolfe and Hermanson (2004) built upon Cressey's (1950; 1953) model by adding (4) capability as a fourth essential element, creating the FDT. They state that the capability to conceal relies upon the fraudster having the personal traits and abilities to commit fraud, and that without these, even in the presence of pressure, opportunity and rationalization, an individual will not commit fraud. Schuchter and Levi (2016) revisited Cressey's (1950; 1953) original FTT to find that the convicted fraudsters they interviewed did not relate to the rationalization of their fraudulent behaviour, but rather identified this as a 'fraud inhibiting inner voice' that becomes quieter over the time the fraud took place. Likewise, Marks (2012) builds upon the FTT adding two components, capability and arrogance, to develop the Fraud Pentagon Theory (FPT).

Cressey's (1950; 1953) work, and therefore later iterations of the model proposed by Wolfe and Hermanson (2004), Marks (2012) and Schuchter and Levi (2016) are based on two assumptions: (1) that individuals accepted their initial work-based responsibilities in good faith (they did not seek out opportunities to defraud), and (2) circumstances in their lives made them violate the trust given to them within their role. These theoretical assumptions have permeated fraud theory since the 1950s and assume that fraudsters are opportunistic. This demonstrates the constraints of the fraud triangle, and later iterations, in that they only focus on the 'insider threat', viewing fraudsters as otherwise law-abiding individuals who have turned criminal, rather than organized criminals who purposefully seek out opportunities to defraud.

> Trust violators, when they conceive of themselves as having a financial problem that is non-shareable and have knowledge or awareness that this problem can be secretly resolved by a violation of the position of financial trust. Also, they are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property (Cressey 1953: 742).

Whilst much fraud theorization has focussed on this narrow conception of the fraudster, and particularly white-collar criminals and 'professional enablers' (Levi 2020), others have considered wider causal explanations of fraud. Indeed, as Nettler (1974) noted in a critique of an all-encompassing theorization of criminality, social systems are complex, and people are motivated by a diverse range of factors that are far from universal or singular. Moving away from the position that fraudsters begin as law-abiding citizens, scholars have considered those who

actively seek out opportunities to defraud, and who are often a fundamental part of serious organized crime (Levi 1981; 2008; May and Bhardwa 2018). Levi's (2008: xxii) study of 'long firm fraud' provides what he describes as 'early forms of "rational choice" and "routine activity" theory' by considering how different people subjectively construct crime opportunities in their environment. This work demonstrates the pre-planned and organized nature of this type of fraud for some fraudsters, as well as how particular situations can enable fraud. Kranacher *et al.* (2010) offered a motivation-led model, suggesting that the presence of the differing forms of motivation in the acronym MICE (money, ideology, coercion and ego) is needed for fraud to occur. Likewise, Vousinas (2019) put forward the S.C.O.R.E model (stimulus, capability, opportunity, rationalization and ego), by building on the FDT, and introducing the concept of ego. Raval (2018) attempted to shift the focus of the FTT and FDT to a disposition-based fraud model that views executive fraud as an act of indulgence. In contrast, personality traits and a person's cognitive reasoning have been identified as a potential strong predictor of a person's intention to commit fraud (Maulidi 2020). Arguably, this links to the ABC model proposed by Ramamoorti *et al.* (2009) which identifies that fraudsters are 'bad apples' and commit fraud in collusion with others (bad bushel) and informed by wider cultural factors that enhance or permit fraud (bad crop).

In contrast, Burgard and Schlembach (2013) approach an understanding of fraud from a different perspective, by examining the structures and processes that are involved in fraud, cyber fraud in particular, through Goffman's (1974) concept of frame analysis. This concept is also used in cybercrime research by Freiermuth (2011) to analyse the strategies of email scammers.

> When two people play chess, for example, they observe the game with two different frames of reference: a *physical* frame, which enables the players to move the figures on the chess board through space and time, and a *social* frame of the game, which determines the rules and the possible and favourable moves of the figures (Burgard and Schlembach 2013: 113).

Frames are deemed a 'strip of reality' (Burgard and Schlembach 2013). When two people interpret a frame in the same way, that becomes a shared reality and a frame of reference. As such, both individuals can play chess together. Goffman (1974) identifies that two types of transformation are available within a shared frame; a key, where transformations are shared, and a fabrication, where one person is in control of the transformation (Burgard and Schlembach 2013).

> A second class of fabrications, the exploitive kind, is now to be considered: one party containing others in a construction that is clearly inimical to their private interests, here defining 'private interests' as the community might (Goffman 1974: 103).

All fraud and deception are considered a fabrication. Burgard and Schlembach (2013) assert that the fraudsters must figure out how to move their victim voluntarily into this exploitative interaction. They suggest that this is achieved in cyber fraud because it is often in the 'private interests' of individuals to engage in this interaction (Burgard and Schlembach 2013: 114). Examples of this can be seen in incentive-based models of fraudulent interactions, where a benefit to the 'victim' entices them to engage (unknowingly) with the fraudster; or fear-based models, that compel 'victims' to engage due to potential loss if they do not (such as fraudsters posing as the victim's bank calling to advise them of a cyber-attack). This work, and that of Maurer and Levi, moves theorizations of fraud away from the 'white collar' fraudster to consider the social interactions taking place during the process of fraudulent behaviour. However, more consideration should be given to theorizing the spatial context within which these social interactions occur. Whilst a limited body of scholarship has considered the environment in which fraud

occurs, the liminal nature of this environment and the performativity of fraudsters in them has yet to be examined through this lens. This paper thus further realigns the academic gaze away from fraudster characteristics, motivations and social interactions to argue that greater consideration needs to be given to the spatial and temporal positioning of fraud. In addition, our novel approach of co-producing theory with experts by experience adds methodological innovation yet to be seen in fraud theorization.

LIMINALITY 'AT WORK'

In organizational literature, liminality is often taken to mean a position of ambiguity and uncertainty (Beech 2011). Shortt (2015) defined liminal space as a space that is on the 'border', a space 'at the boundary of two dominant spaces, which is not fully part of either' (Dale and Burrell 2008: 238). It is a 'no man's land' (Dale and Burrell 2008: 239) that is not easily defined in terms of its use nor 'owned' by a particular party. Liminal space is a space where anything can happen (Turner 1974).

> liminal spaces are nonetheless in direct comparison to dominant spaces; those spaces that are defined by mainstream uses, that characteristically have clear boundaries and where the practices within them are interwoven with social expectation, routines and norms (Shortt 2015: 634)

Liminal space has been considered as a space that facilitates criminal behaviour, such as in the street or the city (Matthews 2003; Hallsworth and Silverstone 2009). Criminologists have focussed on how punishment is experienced (Jewkes 2013), applying the concept to prison and carceral spaces (Moran 2013; Moran *et al.* 2016), or considered the role liminal space plays in the facilitation of rehabilitation and reform (Harding 2020). Others have examined the liminal nature of the night-time economy and the role of bouncers in policing environments where violence and aggression are routine (Hobbs *et al.* 2002; 2003).

Liminality can be used to understand the role of people in guiding others in unknown or unfamiliar locations, settings or procedures. For example, within a rite of passage, such as marriage, the ceremony is overseen usually by the religious or official individual who guides the couple through the process. They offer the structure that guides the transition down its rightful path. This individual, specifically within the liminal space, transforms temporarily to become the knowledgeable actor that guides the more naïve within this space. In Shields' (1991) conception of the Victorian seaside as a liminal space, the role of those in charge of bathing machines and in assisting bathers was identified as 'mediaries between two worlds', the 'civilised lands and the undisciplined waves'. They were the knowledgeable actors within this interaction, within this liminal space; to the dippers, they 'were essential figures of dependable strength and assurance' (Shields 1991: 85). The knowledgeable actor offers structure within an uncertain and ambiguous space where social rules and norms are undefined or in a state of flux.

Arguably liminality, whilst not explicitly identified as such, is evident in the works of Goffman and Maurer when they explore the ways fraudsters engage in a performance and lead targets through the process involved in what, for victims, may be an unfamiliar investment scenario. Fraudsters in Goffman and Maurer's work, guide targets through these unfamiliar procedures, and enact the role of the 'Confidence Man' to persuade targets to hand over their money. This body of work illustrates the social engineering techniques employed by organized crime groups to defraud persons. In both cases, the fraudster engineers social situations to entrap the target, thereby creating a 'liminal context' or situation by the opportunity they falsely create. More often today, however, victims engage in liminal spaces and contexts not engineered by fraudsters,

but instead are manipulated by fraudsters who use them to enact their liminal identity. In some instances, fraud is committed in physical or virtual spaces, as in Maurer's research, in what could be defined as 'offender convergence settings' (Felson 2003), and a liminal context is created by the fraudster in this venue: the unfamiliar bogus business opportunity.

Taking the role of a knowledgeable actor and creating a liminal context involves constructing a liminal identity, by becoming a shape-shifting chameleon. In Maurer's (2000) research, this identity is that of the confidence man in an investment or business opportunity falsely constructed by the fraudster. This is one example of the social engineering techniques fraudsters employ, and how they present themselves as capable guardians. Liminal spaces are manipulated to execute social engineering techniques, such as creating a liminal identity and assuming the role of a capable guardian. Goffman's (1963) work on identity construction is useful here. Through his concept 'dramaturgy', Goffman asserted that social life is like a never-ending everyday theatre in which we are actors. From birth, we are socialized to learn our assigned roles in the theatrical play, and that of others. People engage in impression management, controlling how we appear to others and the ways we act in particular settings. As he explains, individuals construct a 'front stage' persona or appearance in everyday interactions when they know they are being watched by others, and this can be different to the 'backstage' when people are more relaxed, uninhibited and act as their true self. Goffman's work on stigma demonstrates how identity construction entails self-presentation and the management of verbal and visual impressions (Goffman 1959, 1963). The construction of identity is therefore understood as an 'active process of taking certain subject positions in an on-going process of becoming – rather than merely being – in the world' (Jackson 2004: 674). Liminal spaces, because they are often unfamiliar, unclear or unknown, provide those within them to take on or enact different identities: the educator, the guide and the facilitator. Noble and Walker (1997) describe how liminality 'significantly disrupt[s] one's internal sense of self or place within a social system' (31). As such, liminality can be defined as 'a reconstruction of identity in such a way that the new identity is meaningful for the individual and their community' (Beech 2011: 287). The rules of the game and social rules are not always apparent in these spaces because of their unfamiliarity, thereby enabling fraudsters to reconstruct their identity as a knowledgeable actor.

CO-PRODUCING THEORY

This paper is a theoretical paper based upon various forms of knowledge, including the subjugated knowledge of the ex-fraudster. Co-written by academic researchers, an ex-fraudster, a former police leader in fraud and economic crime and current practitioners within fraud prevention, this article applies a holistic and co-produced approach to the production of theory. The decision to take this approach is an acknowledgement of how we often prioritize certain types of knowledge ('official' knowledge) and certain types of knowledge producers (researchers/practitioners) which leads to a replication of certain ideologies (Smith 2012; Naples and Gurr 2014). In traditional academic enquiry, epistemic authority and epistemic privilege can work together in a symbiotic relationship to conceal rather than discover (Harding 2020). Epistemic authority speaks of 'whose knowledge is recognized and validated and whose is silenced' (Naples and Gurr 2014: 21). The ex-fraudster very rarely holds epistemic authority despite being the most knowledgeable actor regarding the mechanics of fraud itself. This is because they are denied the epistemic privilege of being referred to as authorities in fraudulent activity, regardless of the skills and expertise built during a criminal career as a fraudster within an organized crime network. Police and crime prevention experts have less of a challenge directing research due to the epistemic privilege that is extended by their current and previous job titles, yet there is still often a lack of presence within criminological research on fraud and financial crime. Within this

paper, we call upon all the lived, learned and professional expertise of the authoring group to offer a well-rounded and holistic perspective of fraud.

The co-production of this paper took place over 3 years and was an iterative process, involving multiple discussions about existing academic theory. Theorization emerged from these discussions organically rather than theory development being a planned output of our dialogues. We explicitly engaged with theory development, identifying current approaches and gaps in knowledge. This was mostly done in a workshop-style format with mind mapping activities and practical application of the theory to existing case studies of fraud prevention strategies, both conducted by co-authors (e.g. see Harding and Cooper 2021) and other academic research (cited throughout). Team members would constructively critique each other's perspectives, drawing from our expertise in fraud perpetration, fraud prevention and investigation and academic research. Whilst there is extensive literature exploring the co-production of research, this often pertains to data collection and analysis of data rather than theory production. We advocate that theory production, particularly when it applies to crime prevention, should include those with lived experience of all aspects where possible to maximize its practical impact. Moving forward, future collaborations on theory development may seek to draw upon co-production approaches that have used a step-by-step approach (Vargas *et al.* 2022) or framework to co-production (Hawkins *et al.* 2017), hosting co-design pre-planned agenda-led events (Farr 2018) and may consider the co-design development of theory to be at certain stages of development, from inception, through to consultation at later stages of theorization.

IDENTIFYING LIMINALITY IN FRAUD

Fraud occurs in a variety of physical and virtual spaces and contexts, and in several different ways. Fraudsters need the in-between-ness and ambiguity of liminal space or contexts to facilitate the deceptive transaction. This paper offers three examples of fraud. Firstly, fraud that involves an organization as a victim (invoice fraud), then an individual as the victim (traditional romance fraud), and finally an emerging case of transforming a victim of romance fraud (individual) into a co-offender/accomplice, in re-focussing the target of the fraud from the individual to an organization (recruiting a data mule via romance fraud). These fraud types were chosen because they effectively demonstrate the role of liminal spaces and liminal identities in fraud perpetration, represented a breadth of expertise that the team possess, and offer a range of victimization demographics and mediums (such as digital and in-person) to illustrate the theory's applicability.

Invoice fraud

Fraud against an organization or business occurs most commonly through business email compromise (BEC) (Agari 2020). BEC fraud is sometimes also referred to as cyber-enabled financial fraud (Cross and Gillett 2020), chief executive officer (CEO) fraud, spear phishing, whaling (Gupta *et al.* 2017), whale-phishing, email spoofing (Kruck and Kruck 2006) and email account compromise (Symantec 2019). Meyers (2018) explains how BEC that results in full account take over and invoice fraud is not simply a cyber-attack but fraudulent behaviour that 'normally relies on social engineering techniques, such as knowledge of the targeted person or organization, exploitation of business hierarchies or dynamics and multimedia interactions (such as following up on an email with a telephone call)'. Cross and Gillette (2020) identify that fraudsters use social media platforms such as LinkedIn to gather intelligence about a company that may allow them to successfully infiltrate and imitate an aspect of or an entire company. As such, a BEC enables invoice fraud and relies upon liminal identities within the virtual business relationship as much as gaining access to a key email account within the organization.

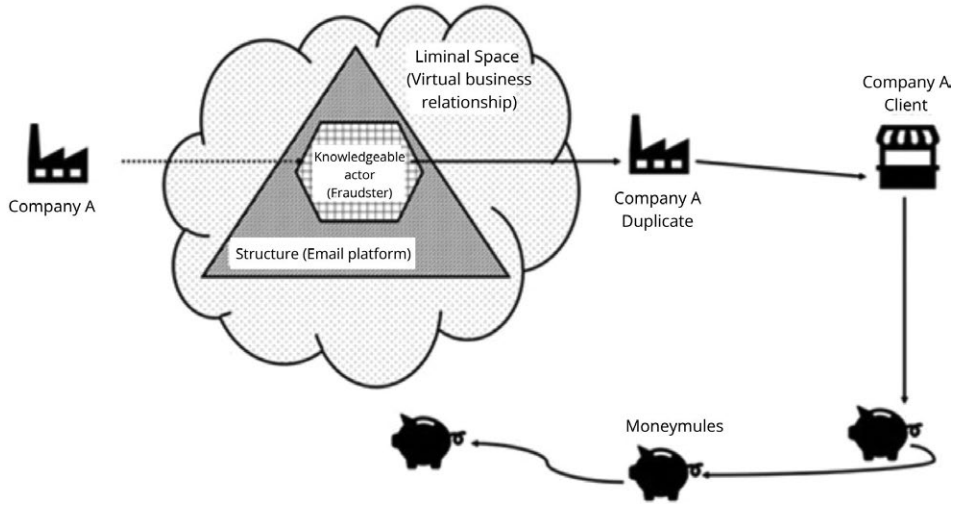

Fig. 1 Invoice fraud and liminal space

Here, the process of BEC and invoice fraud within a liminal space is presented. In Figure 1, Company A uses an email platform as a way of communicating digitally in a structured way within the liminal, less structured, space of the virtual business relationship. A virtual business relationship is one that primarily exists online. Perhaps the individual worker has never met the client in person, and rarely deals with them over the phone; prominent ongoing communication is by email. Interpol (2022) has sought to raise awareness of BEC fraud, where social engineering tactics are used to gain information about corporate payment systems, and then deceive company employees into transferring money into their bank account. When a fraudster infiltrates the structured email platform, they become a knowledgeable actor. This can occur through weak passwords, malware or access granted through phishing emails, or by phishing messages on social media websites and apps such as LinkedIn. Email server access can also be gained through physical access to office buildings.

Once email account access has been gained, criminals can then view all account activity, such as past saved emails, sent emails and emails received. With this access and open-source intelligence (OSINT)[2] gathered from sources such as social media accounts and the organization's website, the fraudster intercepts emails and, using social engineering, sends out fraudulent emails posing as Company A. In essence, the fraudster acts as a duplicate of Company A. They become the knowledgeable actor, controlling information flows between the duplicate Company A and the outside world, including their clients. This can be referred to as a 'man in the middle' (MITM) attack vector through 'email hijacking'. Whilst MITM can span numerous attack styles, the fraudster will likely use other methods often from their OSINT toolkit to form an idea of their victims (both Company A and their clients) prior to engaging in any communications. The fraudster then begins sending out invoices that appear to be from the company but redirects payments to money mule accounts held by the fraudster.

Virtual business relationships, because of their online and non-face-to-face nature, provide fraudsters with the opportunity to intercept and compromise business emails. During the past year, as more people around the world have been home working due to the Coronavirus disease 2019 (COVID-19) pandemic (ONS 2022), BEC has risen dramatically (Minnaar 2020). This is

2 See this useful OSINT framework opensource toolkit https://osintframework.com/ for more details.

because we have become more reliant than ever on virtual business relationships, putting more of our daily and previously face-to-face interactions online that are easier for fraudsters to intercept or gather data, which can then be used to impersonate. Within a BEC attack that results in invoice fraud, it is the virtual business relationship that creates the liminal space within which fraud can occur. The structure within which the worker(s) of Company A believe themselves to be working in, is a secure email platform. They are not suspicious of others having access as they assume the structure of the email platform affords them safety by the use of passwords to access and spam email filters within the platform. Yet the virtual business relationship spans various platforms, such as social media (LinkedIn, Yammer, etc.), websites, and other communication applications such as Microsoft Teams. These spaces are each structured and regulated by their own terms and conditions with no overall oversight and as such become 'in-between' spaces within which virtual business relationships are fostered and developed. Information that is shared in these spaces constructs the virtual business environment as a liminal space, where information that is exchanged can facilitate invoice fraud by concealing fraudulent activity.

Romance fraud

Dating is perhaps far simpler to conceptualize as occurring in liminal space as it is the beginning stage of an adult rite of passage that has already been theorized within anthropological literature (Ben-Ze'ev 2004). Dating apps are used worldwide, with estimates that there are over 200 million apps (Castro and Barrada 2020) some with international reach (e.g. Bumble, eHarmony, Match, Tinder). In contemporary terms, 'online' dating is where an individual signs up for the dating app with the purpose of making a romantic match. They view the app as facilitating the transition from being a single individual to a couple in a romantic relationship. In this way, the app facilitates one of the 'rites of passage' identified with liminal space: the threshold of a transition in life stages. Whilst dating apps are highly structured to facilitate making a romantic match, the liminal space of online dating spans online and offline worlds, in that the relationship will begin online with the hope that it will continue to develop in person.

The actions within the app are designed to connect users and facilitate romantic communication, following its own terms and conditions of use, and structured functionality that assumes that everyone using the app is there for the purpose of dating. However, the fraudster as the knowledgeable actor is drawn to the dating app as a way of eliciting a financial exchange rather than a romantic one. Taking on the temporary liminal identity of an online dater, the fraudster will use social engineering techniques designed to evoke emotional responses that masquerade as an intimate relationship (Ma and McKinnon 2020). The fraudster 'must strike a balance between the romantic and financial aspects of the communication for their criminal intent to remain hidden' (Carter 2021: 283). Once a 'relationship' is developed, the fraudster will shift the relationship from being based on romance to being based on economic manipulation. The romantic target then becomes a victim of romance fraud. Figure 2 demonstrates how it is the presence of the fraudster, with full knowledge of their own agenda, that interrupts the rites of passage from a single individual to part of a couple.

The liminality of online dating obscures the true identity of the fraudster, or even the fact that it is a fraudster and not a genuine romantic match. Carter (2021) highlights the difficulty that fraudsters face 'maintaining a romantic façade whilst advancing the concealed goal of extorting money and mitigating talk potentially incompatible with romance, such as financial matters, urgency and secrecy'. This may also be challenging if there are time differences, should the fraudster be based in another country, or because of a lack of awareness of cultural cues or knowledge. It is only through the ambiguity offered by the liminal space of online dating that the liminal identity of a potential love match can be balanced with the conflicting agenda of financial extortion.

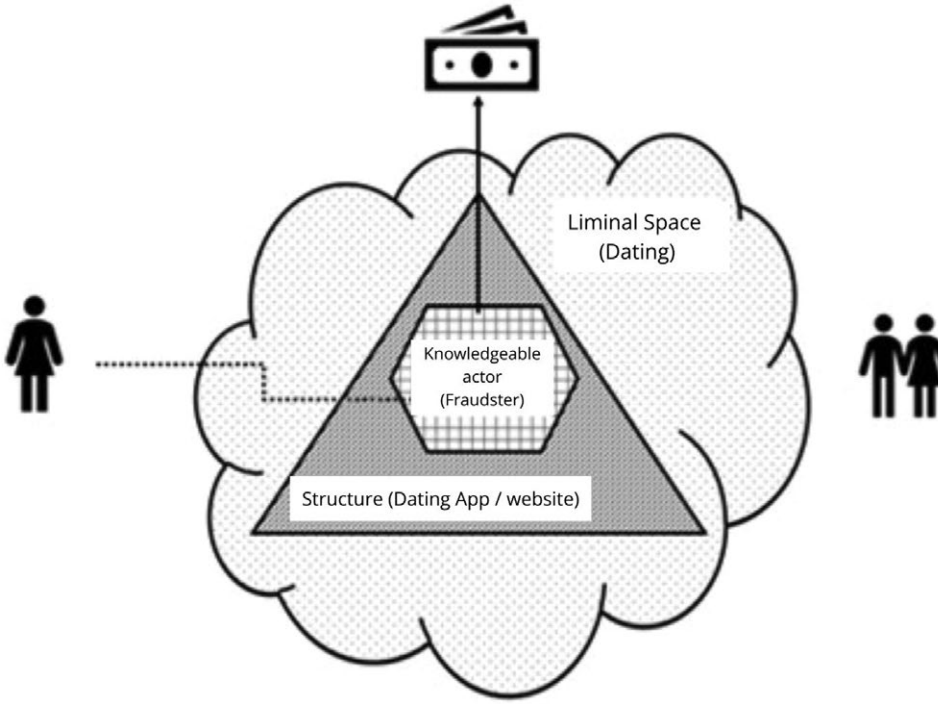

Fig. 2 Traditional romance fraud

Fraud is commonly understood as deceptive activities designed to achieve financial gain. However, in the digital information age, obtaining personal and company data has more recently become a potentially more valuable outcome of fraudulent activity. Figure 3 shows how romance fraud can be used as a gateway to obtain various forms of financial gain through obtaining company data or the personal data of others held by the romance fraud victim's employer.

The romance fraud threat depicted in Figure 3 adds another dimension to previous conceptualizations of romance fraud, that saw romance fraud only ever as an attack against the individual. Here, we show how individual liminal spaces can be transformed into opportunities to target organizations through its staff. Using the same OSINT gathering discussed in Figure 1, fraudsters can use social media dating, or dating-specific apps to target strategic members of staff. Dating apps often share the names of employers, roles within an organization, geographic location and other characteristics that allow fraudsters to make strategic approaches via online dating apps. Utilizing information freely available on social media, the fraudster can emulate characteristics of the victim's ex-partners in their liminal 'dater' identity and can make pinpointed and targeted attacks on specific individuals in specific organizations for specific forms of data. They will use the liminal space of the dating app not to defraud the immediate online dater, but to recruit them as a company 'insider threat' or data mule. The online dater's employer is then the overall victim, with the online dater criminally exploited by the fraudster.

Even when not purposefully targeted, users of dating apps give away personal information about their location, employer and job titles in their biographies. Metadata/EXFI data from images and videos can give precise locations and models of the device used to take the image, which can then be utilized to design an attack specific to the known vulnerabilities of that device. Fraudsters can develop infected files to be sent to the victim, then socially engineer them

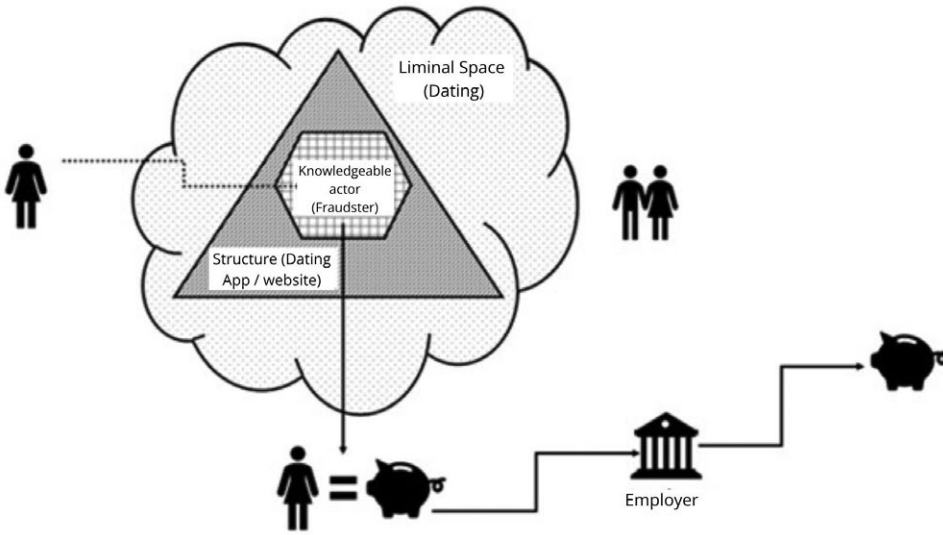

Fig. 3 Romance fraud to recruit 'insider threat' or data mule

to open them, compromising the device. This is a particular risk to businesses where they allow BYOD (bring your own device), with staff members accessing dating sites alongside sensitive business data on the same device.

A fraudster can easily set their location to target-specific industries, such as banking, by setting their location to a small radius in the financial districts of any major city. This will show up individuals who are working in nearby offices during the working day. During the COVID-19 pandemic, the internationally popular dating app Tinder allowed users to set their own location anywhere in the world, offering opportunities for fraudsters to target areas far away from their own location. This removed a potential distance barrier that might have blocked engagement previously, as the online dater may chose not to engage in a potential long-distance love match.

Fraudsters engaging in romance fraud via online dating apps will mostly attack in high volumes, knowing that uptake from daters who are willing to part with money will be low. For example, one convicted fraudster, Osagie Aigbonohan, contacted over 670 people on dating sites Tinder and Plenty of Fish before successfully scamming women out of over £20,000 (Vesty 2022). Some fraudsters use dating apps to target-specific organizations, usually as part of a much larger organized crime operation against an organization. Therefore, it is a lower volume and more time-consuming form of romance fraud. Yet the rewards are potentially far greater. In the same way that organized fraudsters use the liminal space of the virtual business environment, via apps and websites such as LinkedIn in the invoice fraud example demonstrated in Figure 1, the same fraudsters are able to use the liminal space of social media and dating websites to target staff of business using romance fraud or sextortion tactics to influence business decision-making, obtain data or other forms of bribery and corruption, such as opening bank accounts without identification.

PUTTING LIMINALITY INTO FRAUD PREVENTION PRACTICE

Understanding the utility that liminal spaces provide online fraudsters can help reposition law enforcement, businesses, individuals and policy makers as knowledgeable actors. According to Kleemans *et al.* (2012: 87) 'If crime needs the convergence in time and space of a motivated

offender, a suitable target, and absence of a capable guardian (the "crime triangle"), this means that crime can be prevented by keeping motivated offenders away from suitable targets at specific points in time and space or by increasing the presence of capable guardians'. This knowledgeable position can enable practitioners to protect, deflect and steer 'naïve' users away from the exploitative actions of other knowledgeable actors, such as the fraudster. To do this, we have proposed that a better understanding of liminal spaces and how they offer fraudsters the ability to construct a fake identity and manipulate users is needed within crime prevention strategies. Liminal spaces, whilst they are out there, nowhere, physically unplaced, invisible, and for some unimaginable, are environments that can be manipulated to increase the risks and efforts needed to successfully commit fraud. This paper extends Burgard and Schlembach's (2013) approach to understanding fraud interactions using Goffman's (1974) concept of frame analysis. We argue, that for fraud to occur, liminality must be present. Burgard and Schlembach (2013) analyse the interaction within the frame, but we identify the frame as a liminal space.

The interaction observed by Burgard and Schlembach (2013) will be dependent upon the fraud model used by the criminal, which is often dictated by the liminal space within which the fraudster occupies. Crucially, the fraud models in Table 1 demonstrate the motivation of the (potential) victim to engage with the fraudster as a knowledgeable actor within a liminal space, not the motivation of the fraudster as seen in previous models (Cressey 1950; 1953; Ramamoorti 2008; Kranacher *et al.* 2010; Schuchter and Levi 2016). Rather, these are the 'hooks' that fraudsters use to socially engineer victims of fraud depending upon the circumstances and spatial context of the exchange between fraudster and (potential) victim.

Environmental perspectives of crime could therefore be harnessed to reshape offender decision-making and patterns of victimization (Clarke 2008; Freilich *et al.* 2019). These perspectives take a place-based crime prevention approach because it is believed crime is a result of opportunities created by the environment, and temporal and spatial elements of liminal spaces. Levi's (2008) suggestion that routine activity theory can be applied to fraud is useful here, as this approach is concerned with the ecology of the crime environment and its opportunity for crime (Cohen and Felson 1979; Felson and Cohen 1980). According to routine activity theory, three components' offenders, targets and places are necessary conditions for crime to occur (Felson 2008). Crime is highly likely if offenders meet targets without the presence of an effective controller, such as a capable guardian (e.g. security guard, police). Thus, crime prevention approaches have sought to increase the number of controllers or increase their effectiveness

Table 1. Fraud models

Fraud model	Example
Incentive based	Victim responds to advert for a discounted product or service, such as a loan, pays a fee but does not receive the product, such as advance fee fraud or submits their details to a spoofed website.
Fear based	Fraudsters will spoof the phone number of a victim's bank and telephone them and make them believe that they are currently a victim of a cyber-attack and they need to transfer their money now or lose it to criminals.
Desire based	Approaches to potential victims on dating sites to get 'gifts' or 'borrow' money from potential suitors (romance fraud), or explicit and/or embarrassing pictures and/or videos are obtained from romantic interests which are then used to extort money and other valuable material from the victim (sextortion).
Vulnerability based	Poor email password practice leads to BEC, fraudsters take advantage of this vulnerability.

(Sampson *et al.* 2010). Our work enhances routine activity theory explanations, by emphasizing the liminal nature of the spaces where offenders and targets meet, and the liminal context and identity created by the fraudsters in those settings. We argue that liminality is a key factor in understanding how fraudsters can exploit targets in those spaces.

SCP techniques, which have been developed from three theoretical perspectives (see Smith and Clarke 2012), may also offer a means to manage risks in liminal spaces and deter fraudsters who may exploit them. Leading SCP scholars Cornish and Clarke (2003) have proposed 25 techniques that can be used to reduce the opportunity for crime to be committed. These techniques are categorized under five SCP strategies: increase the effort, increase the risks, reduce the rewards, reduce provocations and remove excuses. SCP have been utilized to deal with a range of crimes such as sexual offences (Cook *et al.* 2019; Krone *et al.* 2020) terrorism (Freilich *et al.* 2019) wildlife crime (Viollaz *et al.* 2021) and theft (Stickle *et al.* 2020). At the core of these approaches is the need to manage and manipulate the context or space where such crimes occur to achieve effective crime reduction. In the context of fraud, we argue that an understanding of the liminal spaces or context in which fraud takes place is critical to reducing fraud victimization.

By synthesizing the theoretical knowledge generated in this paper, and drawing on our lived experience, we developed Cornish and Clarke's SCP techniques for the purposes of fraud prevention. Table 2 shows how SCP techniques can be used to manage liminal spaces more effectively, thereby managing who has access and how to manage the space itself.

Five main themes carry through the application of SCP style prevention tactics applied to the four different fraud models: raising awareness, the appropriate use of technology, vulnerability testing, regulation and securing access to data. Whilst these themes may manifest as different crime prevention products, policies or procedures in different contexts, they broadly map on to the five principles of SCP.

(1) Increase the effort, by raising awareness

This is achieved overall by making people more aware of how fraud occurs and the virtual and physical spaces that they may be particularly vulnerable to criminal approaches, as well as the contexts (e.g. business investments). Examples could include public awareness campaigns (such

Table 2. Fraud models and SCP response

	Fraud model	Example	SCP
Liminal space	Incentive based	Spoofed website	Detect, report, remove spoofed websites. Check site has a valid certificate like SSL (verifying that the web address belongs to the company). Build awareness.
	Desire based	Romance fraud	Stop BYOD; only use company devices for work. Social media usage policies. Regulation of dating apps to ensure adequate KYC (know your customer) procedures in place). Build awareness.
	Vulnerability based	BEC	Stronger passwords/multifactor authentication. Social media usage policies. Regular vulnerability testing. No name policies. Build awareness.
	Fear based	Extortion	Build awareness. Confidential reporting methods.

as Take 5 to stop fraud[3]), staff training, or by specialist provision for those working within compliance and regulated roles. This must be meaningful engagement, not just tick-box training, or inconsistent messaging. Rarely do awareness campaigns address the liminal as too often the visible is targeted because it is easier and often the most vocal get prioritized by the police, government and other key decision-makers. As such, awareness is only raised to superficial levels, reinforcing the role of the knowledgeable actor within liminal/marginal spaces within which fraud occurs. Indeed, as Nettler (1974: 76) noted 'lectures on "borrowing is stealing" are likely to provide weak armour against the great gamut of desires and opportunities for taking other people's money'. Likewise, campaigns to increase hand washing in India have had marginal effects on hygiene changes (Seimetz *et al.* 2016). To move beyond the superficial, awareness-raising initiatives need to be ongoing (Qian *et al.* 2022), given the changing nature of fraud offences. They may be more effective when using a problematizing or deproblematizing frame (Van Gorp and Vyncke 2021) where fraud is presented as a problem or concern, or safety strategies to prevent fraud are promoted. Examples could focus on liminality, asking provoking questions such as 'Do you know for sure you are talking to your bank?', or the positives of employing safety techniques: 'Mary prevented her life savings of £75,000 from being stolen by not transferring money to people she has never met in person'.

(2) Increase the risks, with the appropriate use of technology

There is an abundance of fraud prevention products within the global technology landscape, ranging from AI and machine learning applications designed to identify fraud within open banking data, to biometric identity verification to ensure that your customer is who they say they are. Such approaches assist by mitigating liminal identities. Appropriate use of technology can increase the risk of the fraudster getting caught. Here, technology can become the knowledgeable actor or capable guardian within the liminal space by moderating keywords or denying access when identity cannot be confirmed. However, the use of such technology can often be viewed as a costly 'nice to have' rather than a 'must have' due to lack of regulation. For example, online dating app users are not required to validate their identity using official identity documents, just an email address with an optional 'selfie' to confirm the user shares a likeness to their photographs on some apps.

(3) Reduce the rewards, with secure data storage and encryption

Definitions of fraud have advanced over the years to broaden the scope. In the IIA (2017) definition below, the primary focus is still to seek financial gain through the prevention of loss, financial or property gain or advantage.

> Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage (IIA 2017).

However, the focus on the financial or physical property has meant until 2007, data were not considered of value to criminals. That changed when criminals impersonating policemen stole more than $4 million in equipment from a Verizon Business data centre in northern London during 2007 (Miller 2021). Yet it would be years later that the fraud prevention world would

3 https://www.takefive-stopfraud.org.uk/

begin to realize the worth of data to criminals as well as businesses. The reward now for criminals is not only the financial gain they may be able to immediately make, but the value of the data that they can obtain through ransomware attacks or by recruiting insider threats/data mules. By making data much harder to access, such as only ensuring that relevant staff have access, rather than the whole organization, and ensuring that data are stored securely, ideally with encryption, the rewards for the criminal are reduced, whilst also protecting the business and clients from data loss.

(4) Reduce provocations, by vulnerability testing

Being able to spot vulnerabilities for a criminal is a provocation. Heavily structured, institutional spaces have policies and practices that prompt the surveillance of capable guardians, reducing vulnerabilities. But liminal spaces can be found at the edges: physically, in reception, waiting rooms, etc.; and online, via email systems, dating platforms. These spaces are vital points of ingress and egress for companies and as such have higher levels of third parties, less regulation and less surveillance: the ideal provocation for a fraudster. The only way to truly identify and implement SCP techniques appropriately is to employ vulnerability testing that looks 'through the eyes of a criminal'. That requires the use of lived experience within penetration testing, vulnerability testing and 'red teaming[4]'. Those with experts by experience can draw on their knowledge and experience to identify and establish liminal spaces and contexts within a business. For example, creating liminal identities in settings where identities have yet to be confirmed or are ambiguous, in places where transactions take place. For instance, a multinational Hong Kong based company lost £25 million when an employee transferred money during a deep fake video conference call (Chen and Magramo, 2024). Testing vulnerabilities such as these created by liminal spaces can prevent future financial losses.

(5) Remove excuses, by enforcing the regulation of liminal spaces

Due to the harm felt by fraud and financial crime, it is everybody's problem; however, often it is also nobody's responsibility. This is because fraud needs liminal space to occur, and liminal spaces are under-regulated, in-between spaces that are void of any real ownership or responsibility. Structured systems such as email platforms, dating apps and business policies and procedures create a structure or framework within which people interact. These structures have 'rules' that prompt people to act in specific ways within them to achieve the aim of the space. Such 'rules' prompt human interaction rather than police it, with very little regard for how they interact with the criminal element. Therefore, the fraudster will subvert these 'rules' and utilize them to help commit their crimes just because they can.

The Financial Conduct Authority (FCA) is the regulator of the UK financial services sector. They have the authority to regulate the activities of financial firms around anti-money laundering (AML), counter-terrorist financing (CTF) and bribery and corruption (B&C). The FCA has a global impact by its membership of the Financial Action Task Force (FATF), the Organisation for Economic Co-operation and Development (OECD) and the International Monetary Fund (IMF) (FCA 2023). The FCA implements government legislation that seeks to prevent key areas of serious organized crime such as money laundering by ensuring compliance

4 Red Teaming (RT) is a process whereby a Blue Team represents the intent, objectives and interests of the friendly force, whilst enemies are represented by a Red Team. 'By having a Red Team emulate enemies and reproduce their motivations, intentions, behaviours and anticipated actions, the Blue Team can (1) test and evaluate its own course of actions; (2) identify possible opportunities to exploit weaknesses of the Red Team and thereby the enemies; (3) learn to appreciate the dynamics of how Blue and Red interact and gain an understanding of the space in which the dynamics may unfold and evolve' (Abbas *et al.* 2011: 2).

with a national regulatory standard of practice. Failure to comply can result in significant punishment and fines. However, there is currently no such regulation attached to fraud and financial crime, nor is there regulation beyond the financial services sector.

The Economic Crime and Corporate Transparency Act (Gov.UK 2023) makes 'failure to prevent fraud' an offence in the United Kingdom. It holds organizations to account if they profit from fraud committed by their employees, with the prosecution leading to a potentially unlimited fine. However, organizations can avoid prosecution if they have 'reasonable procedures in place to prevent fraud' (Gov.UK 2023). This means that companies beyond the financial services sector must do more to prevent fraud and financial crime, which could include greater mandatory regulation of sectors that are currently unregulated, such as social media and dating apps. However, guidelines of what this may look like, who will enforce it and how this will be enforced are yet to have been considered. It is unlikely that such regulation, unless deliberately directed to do so, will offer much-needed regulation to the liminal spaces within which fraud proliferates. It is essential that liminal spaces are also considered in such policy and practice with accompanying SCP techniques.

Whilst SCP approaches focus solely on the situated context of crime and not the backgrounds of individual offenders, we do not discount the importance of individual motivations and wider contextual factors that may lead someone into committing fraud. Indeed, much research has rightly identified international structural inequalities such as poverty and inequality, and how some offenders themselves may be vulnerable and the victims of biased political and economic systems (Webster 2023). Likewise, SCP may be limited when dealing with crimes motivated by emotive issues and undertaken for sensations such as thrill-seeking (Hayward 2007). Albeit it is not impossible for someone driven by emotions or seeking to satisfy carnal desires to make rational choices about the risks and benefits of offending. What we are proposing is not a holistic theory of fraud, but a means to understand the situational aspects of fraud that can be harnessed to reduce harm to fraud victims and the risks posed in liminal spaces. Our concern in this paper is an exploration of how fraudsters commit fraud, not what motivates them. Further theoretical work may seek to better understand the interplay between micro, meso and macro theories of fraud to advance current thinking.

We are also not suggesting that it is possible to protect all potential targets of fraud given the vastness of liminal spaces and the expense of doing so. Clarke and Newman (2006) claim that not all targets are at equal risk, with some at greater risk and in need of more protection. However, who determines risk and levels of vulnerability is arguably subjective. Indeed, research by Keay (2023) has shown that police officers struggle to determine who is or who is not vulnerable in crime situations. Further criticism of SCP techniques has also identified the displacement effects of place-based interventions. It is suggested that crimes merely displace and in six possible ways: temporal (change the time of day they commit crime), spatial (move to another location), target (move to another target), tactical (alter the methods used to carry out the crime), offense (move to commit another crime) and offender (new offenders replace old offenders who have been removed or desisted) (Guerette and Bowers 2009). However, research by Hsu and Apel (2015) for example, has shown that displacement may not always occur. Rather, offenders may adapt their techniques and innovate to surmount SCP interventions (Freilich *et al.* 2019).

CONCLUSION

This paper has utilized the viewpoints of academics, practitioners and those with lived experience of conducting fraudulent activity. In this article, we present our theoretical contribution to the field of theories of fraud and build on this theory to establish SCP techniques for fraud prevention. Key SCP thinkers Clarke and Newman (2006) have encouraged those implementing

SCP techniques to deal with terrorism to 'think like a terrorist'. Therefore, should we not also 'think like a fraudster'? We recognize that it is simply impossible to do so. Whilst we may be able to identify some similar thought processes, without lived experience, we argue we cannot fully think like a fraudster. Our thoughts would be merely guesswork, instead of being an expert by experience. Our work goes one step further by co-producing a theoretical article with those who have committed fraud, thereby understanding the steps fraudsters take to commit fraud without the academic guesswork. This collaboration has enabled us to advance theoretical understandings of fraud, to focus on the spatial aspects of fraud. Specifically, this paper has firstly demonstrated that the nuances and complexities of liminal spaces provide fraudsters with the platform to mask, conceal and manipulate their front-stage identity. Through this concealment, fraudsters create a new identity to trick victims into providing access to their material assets or privileged knowledge that could later be exploited. We argue that such a crime cannot be committed without these liminal spaces, where someone is 'in the know' (knowledgeable actor) and someone is not. Through their manipulation of victims' unfamiliarity with such spaces or contexts, fraudsters can extract gains. Liminal identities and liminal space merge to create the conditions for fraudulent activity to occur. This is partly because the fraudster adopts a liminal identity that presents as a predictable or expected actor. Fraudsters create liminal identities during the process of committing fraud. To enact a fake persona that appears legitimate, fraudsters will seek out liminal spaces in person, on the phone or via text message, online or through a combination of communication methods, because they enable liminal identities to be developed. Secondly, we present that fraudsters do not always seek immediate financial gain; the aim of the contemporary fraudster may be personal data which can then be used to commit further crimes. Thirdly, we argue that within liminal space, individuals are transformed into victims of fraud, or potentially in to 'co-offenders' in order to use the individual to target businesses. Finally, we offer several recommendations for businesses and policymakers regarding how the risk associated with liminal space could be reduced. These include raising awareness of the risks posed by liminal spaces, both to organizations' staff and the wider public, in conjunction with the appropriate use of technology. Businesses need to invest in vulnerability testing to ensure that their data, as well as cash, is fully secured and/or encrypted, and greater regulation of liminal spaces needs to occur, either through the organizations own 'best practice' or governmental regulation, if we are to prevent future fraud and financial crime.

REFERENCES

Abbass, H., Bender, A., Gaidow, S. and Whitbread, P. (2011), 'Computational Red Teaming: Past, Present and Future', *IEEE Computational Intelligence Magazine*, 6: 30–42. https://doi.org/10.1109/mci.2010.939578

Adedoyin Isola, L., Johnson Olabode, A. and Muftau Adeniyi, I. (2017), 'Fraud and Business Cycle: Empirical Evidence from Fraudsters and Fraud Managers in Nigeria', *Studies in Business and Economics*, 12: 110–28. https://doi.org/10.1515/sbe-2017-0009

Aftabi, S. Z., Ahmadi, A. and Farzi, S. (2023), 'Fraud Detection in Financial Statements Using Data Mining and GAN Models', *Expert Systems with Applications*, 227: 120144. https://doi.org/10.1016/j.eswa.2023.120144

Agari. (2020), 'The Geography of BEC: The Global Reach of the World's Top Cyber Threat', available online at https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf (accessed 2 April 2021).

Beech, N. (2011), Liminality and the practices of identity reconstruction. *Human Relations*, 64: 285–302. https://doi.org/10.1177/0018726710371235

Bekkers, L., Van Houten, Y., Spithoven, R. and Leukfeldt, E. R. (2023), 'Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands', *Deviant Behavior*, 44: 1368–85. https://doi.org/10.1080/01639625.2023.2196365

Ben-Ze'ev, A. (2004), *Love Online: Emotion on the Internet*. Cambridge: Cambridge University Press.

Buchanan, R. and Shutterstock, T. (2019), *What We Know About Identity Theft and Fraud Victims from Research- and Practice-Based Evidence*. Washington DC: Center for Victim Research.
Burgard, A. and Schlembach, C. (2013), 'Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet', *International Journal of Cyber Criminology*, 7: 112–24.
Button, M., Lewis, C. and Tapley, J. (2009), *Fraud Typologies and Victims of Fraud: Literature Review*. National Fraud Authority.
—— (2014), 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families', *Security Journal*, 27: 36–54. https://doi.org/10.1057/sj.2012.11
Carter, E. (2021), 'Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud', *The British Journal of Criminology*, 61: 283–302. https://doi.org/10.1093/bjc/azaa072
Castro, A. and Barrada, J. R. (2020), 'Dating Apps and Their Sociodemographic and Psychosocial Correlates: A Systematic Review', *International Journal of Environmental Research and Public Health*, 17: 6500. https://doi.org/10.3390/ijerph17186500
Chen, H. and Magramo, K. (2024), "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'". (accessed 10 June 2024).
Clarke, R. and Newmand, G. (2006), *Outsmarting the Terrorists*. Westport, Conn: Praegar Security International.
Clarke, R. V. (2008), 'Situational Crime Prevention', in R. Wortley and L. Mazerolle, eds, *Environmental Criminology and Crime Analysis*, 178–94, Cullompton, UK: Willan Publishing.
Cohen, L. E. and Felson, M. (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, 44: 588–605. https://doi.org/10.2307/2094589
Cook, A., Reynald, D. M., Leclerc, B. and Wortley, R. (2019), 'Learning About Situational Crime Prevention from Offenders: Using a Script Framework to Compare the Commission of Completed and Disrupted Sexual Offenses', *Criminal Justice Review*, 44: 431–51. https://doi.org/10.1177/0734016818812149
Cornish, D. B., and Clarke, R. V. (2003), Opportunities, Precipitators and Criminal Dispositions: a Reply to Wortley's Critique of Stuational Crime Prevention. in M. J. Smith and D. B. Cornish, eds, *Theory and Practice in Situation Crime Prevention, 16, Crime prevention studies*. Monsey: Criminal Justice Press.
Cressey, D. R. (1950), 'The Criminal Violation of Financial Trust', *American Sociological Review*, 15: 738–43. https://doi.org/10.2307/2086606
—— (1953), *Other People's Money; a Study of the Social Psychology of Embezzlement*. Free Press.
Cross, C. (2020), "Oh We Can't Actually Do Anything About That': The Problematic Nature of Jurisdiction for Online Fraud Victims', *Criminology and Criminal Justice*, 20: 358–75. https://doi.org/10.1177/1748895819835910.
Cross, C. and Gillett, R. (2020), 'Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud', *Journal of Financial Crime*, 27: 871–84. https://doi.org/10.1108/jfc-02-2020-0026
Cross, C., Holt, K. and Holt, T. J. (2023), 'To Pay or Not to Pay: An Exploratory Analysis of Sextortion in the Context of Romance Fraud', *Criminology & Criminal Justice*, 0: 174889582211495. https://doi.org/10.1177/17488958221149581
Cross, C. and Layt, R. (2022), '"I Suspect That the Pictures Are Stolen": Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities', *Social Science Computer Review*, 40: 955–73.
Dal Pozzolo, A., Caelen, O., Le Borgne, Y. A., Waterschoot, S. and Bontempi, G. (2014), 'Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective', *Expert Systems with Applications*, 41: 4915–28. https://doi.org/10.1016/j.eswa.2014.02.026
Dale, K. and Burrell, G. (2008), *The Spaces of Organization and the Organization of Space: Power, Identity and Materiality at Work*. London: Palgrave.
Dorminey, J., Fleming, A., Kranacher, M.-J. and Riley, R. (2010), 'Beyond the Fraud Triangle: Enhancing Deterrence of Economic Crimes', *The CPA Journal*, 80: 17–24. www.acfe.com/rttn/rttn-2010.pdf
Dutta, A., Voumik, L. C., Ramamoorthy, A., Ray, S. and Raihan, A. (2023), 'Predicting Cryptocurrency Fraud Using ChaosNet: The Ethereum Manifestation', *Journal of Risk and Financial Management*, 16: 216. https://doi.org/10.3390/jrfm16040216
Farr, M. (2018), 'Power Dynamics and Collaborative Mechanisms in Co-production and Co-design Processes', *Critical Social Policy*, 38: 623–44. https://doi.org/10.1177/0261018317747444
FCA. (2023), 'International Standards and Regulations', available online at https://www.fca.org.uk/about/how-we-regulate/international-standards-regulations (accessed 4 July 2023).
Felson, M. (2003), 'The Process of Co-offending', in M. J. Smith and D. B. Cornish, eds, *Theory for Practice in Situational Crime Prevention*, Vol. 16, 149–68. Devon: Willan Publishing.
—— (2008), 'Routine Activity Theory', in R. Wortley and L. Mazerolle, eds, *Environmental Criminology and Crime Analysis*, 70–7. Cullompton, UK: Willan Publishing.

Felson, M. and Cohen, L. E. (1980), 'Human Ecology and Crime: A Routine Activity Approach', *Human Ecology*, 8: 389–406. https://doi.org/10.1007/bf01561001
Fletcher, R., Tzani, C. and Ioannou, M. (2024), 'The Dark Side of Artificial Intelligence – Risks Arising in Dating Applications', *Assessment and Development Matters*, 16: 17–23. https://doi.org/10.53841/bpsadm.2024.16.1.17
Franks, A. and Meteyard, J. (2007), 'Liminality: The Transforming Grace of In-between Places', *The Journal of Pastoral Care & Counseling*, 61: 215–22. https://doi.org/10.1177/154230500706100306
Freiermuth, M. R. (2011), 'Text, Lies and Electronic Bait: An Analysis of Email Fraud and the Decisions of the Unsuspecting', *Discourse & Communication*, 5: 123–45. https://doi.org/10.1177/1750481310395448
Freilich, J. D., Gruenewald, J. and Mandala, M. (2019), 'Situational Crime Prevention and Terrorism: An Assessment of 10 Years of Research', *Criminal Justice Policy Review*, 30: 1283–311. https://doi.org/10.1177/0887403418805142
Goffman, E. (1952), 'On Cooling the Mark Out: Some Aspects of Adaptation to Failure', *Psychiatry*, 15: 451–63. https://doi.org/10.1080/00332747.1952.11022896
—— (1959), *The Presentation of the Self in Everyday Life*. Milton Keynes: The Penguin Press.
—— (1963), *Stigma: Notes on the Management of Spoiled Identity*. New Jersey: Prentice-Hall.
—— (1974), *Frame Analysis: An Essay on the Organization of Experience*. Oxford University Press.
Gov.UK. (2023), 'Factsheet: Failure to Prevent Fraud Offence' (published 20 June 2023), available online at https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-failure-to-prevent-fraud-offence#how-will-this-impact-businesses (accessed 4 July 2023).
Grabosky, P. and Smith, R. G. (1998), *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Sydney: The Federation Press.
Guerette, R. T. and Bowers, K. J. (2009), 'Assessing the Extent of Crime Displacement and Diffusion of Benefits: A Review of Situational Crime Prevention Evaluations', *Criminology*, 47: 1331–68. https://doi.org/10.1111/j.1745-9125.2009.00177.x
Gupta, B. B., Arachchilage, N. and Psannis, K. (2017), 'Defending Against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions', *Telecommunication Systems*, 67: 247–67.
Hallsworth, S. and Silverstone, D. (2009), '"That's Life Innit": A British Perspective on Guns, Crime and Social Order', *Criminology and Criminal Justice*, 9: 359–77. https://doi.org/10.1177/1748895809336386
Harding, N. A. (2020), Co-constructing feminist research: Ensuring meaningful participation while researching the experiences of criminalised women *Methodological Innovations*, 13. https://doi.org/10.1177/2059799120925262
Harding, N. and Cooper, E. (2021), "A 'Rapid Response' to fraud and financial crime". *The Public Sector Counter Fraud Journal*.
Hawkins, J., Madden, K., Fletcher, A., Midgley, L., Grant, A., Cox, G., Moore, L., Campbell, R., Murphy, S., Bonell, C. and White, J. (2017), 'Development of a Framework for the Co-production and Prototyping of Public Health Interventions', *BMC Public Health*, 17: 689. https://doi.org/10.1186/s12889-017-4695-8
Hayward, K. (2007), 'Situational Crime Prevention and its Discontents: Rational Choice Theory Versus the 'Culture of Now'', *Social Policy & Administration*, 41: 232–50. https://doi.org/10.1111/j.1467-9515.2007.00550.x
Hobbs, D., Hadfield, P., Lister, S. and Winlow, S. (2002), ''Door Lore'. The Art and Economics of Intimidation', *The British Journal of Criminology*, 42: 352–70.
—— (2003), *Bouncers: Violence and Governance in the Night-Time Economy*. Oxford: Oxford University Press.
Hsu, H. Y. and Apel, R. (2015), 'A Situational Model of Displacement and Diffusion Following the Introduction of Airport Metal Detectors', *Terrorism and Political Violence*, 27: 29–52. https://doi.org/10.1080/09546553.2014.962989
IIA's. (2017), 'International Standards for the Professional Practice of Internal Auditing (Standards)', January 2017. The Institute of Internal Auditors, available online at https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf
Interpol. (2022), 'Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams'.
Jackson, A. Y. (2004), 'Performativity Identified', *Qualitative Inquiry*, 10: 673–90. https://doi.org/10.1177/1077800403257673
Jewkes, Y. (2013), 'Loss, Liminality, and the Life Sentence: Managing Identity Through a Disrupted Lifecourse', in A. Liebling and S. Maruna, eds, *The Effects of Imprisonment*. Routledge.
Kapardis, A. and Krambia-Kapardis, M. (2004), 'Enhancing Fraud Prevention and Detection by Profiling Fraud Offenders', *Criminal Behaviour and Mental Health*, 14: 189–201. https://doi.org/10.1002/cbm.586

Keay, S. (2023), '*How do the police define, identify and respond to vulnerability?*'. *PhD Thesis*.
Kleemans, E. R., Soudijn, M. R. J. and Weenink, A. W. (2012), 'Organized Crime, Situational Crime Prevention and Routine Activity Theory', *Trends in Organized Crime*, 15: 87–92. https://doi.org/10.1007/s12117-012-9173-1
Kranacher, M. J., Riley, R. and Wells, J. T. (2010), *Forensic Accounting and Fraud Examination*. Hoboken, NJ: John Wiley and Sons.
Krone, T., Spiranovic, C., Prichard, J., Watters, P., Wortley, P., Gelb, K. and Hunn, C. (2020), 'Child Sexual Abuse Material in Child-Centred Institutions: Situational Crime Prevention Approaches', *Journal of Sexual Aggression*, 26: 91–110.
Kruck, G. and Kruck, S. E. (2006), 'Spoofing – A Look at an Evolving Threat', *Journal of Computer Information Systems*, 47: 95–100.
Levi, M. (1981; 2008), *The Phantom Capitalists: The Organisation and Control of Long-Firm Fraud*, 1st and 2nd edn. Aldershot: Ashgate.
—— (2020), 'Making Sense of Professional Enablers' Involvement in Laundering Organized Crime Proceeds and of Their Regulation', *Trends in Organized Crime*, 24: 96–110. https://doi.org/10.1007/s12117-020-09401-y
Ma, K. and McKinnon, T. (2020), 'COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic', *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3718845
Marks, J. (2012), 'The Mind Behind the Fraudsters Crime: Key Behavioral and Environmental Elements', in ACFE Global Fraud Conference, 1–62, available online at www.crowe.com
Matthews, H. (2003), 'The Street as Liminal Space', in P. Christensen and M. O'Brien, eds, *Children in the City*, 101–7. Routledge/Falmer.
Maulidi, A. (2020), 'Critiques and Further Directions for Fraud Studies: Reconstructing Misconceptions About Developing Fraud Theories', *Journal of Financial Crime*, 27: 323–35. https://doi.org/10.1108/jfc-07-2019-0100
Maurer, D. W. (2000), *The Big Con: The Story of the Confidence Man and Confidence Trick*. London: Arrow Books Limited.
May, T. and Bhardwa, B. (2018), *Organised Crime Groups Involved in Fraud Crime Prevention and Security Management*. Palgrave, available online at http://www.palgrave.com/series/14928
Meyers, A. (2018), 'Not Your Fairy-Tale Prince: The Nigerian Business Email Compromise Threat', *Computer Fraud and Security*, 2018: 14–6. https://doi.org/10.1016/s1361-3723(18)30076-9
Miller, R. (2021), 'Foiled Plot to Attack Amazon Reflects Changing Nature of Data Center Threats'. *Data Center Frontier*.
Minnaar, A. (2020), ''Gone Phishing': The Cynical and Opportunistic Exploitation of the Coronavirus Pandemic by Cybercriminals', *Acta Criminologica: African Journal of Criminology & Victimology*, 33: 28. https://journals.co.za/doi/abs/10.10520/ejc-crim-v33-n3-a3
Moran, D. (2013), 'Between Outside and Inside? Prison Visiting Rooms as Liminal Carceral Spaces', *GeoJournal*, 78: 339–51. https://doi.org/10.1007/s10708-011-9442-6, available online at https://www.jstor.org/stable/pdf/42006323.pdf?casa_token=3Qh6hxf61iYAAAAA:wgL6qVb5pT9DnTHfTnL-RlqAVyt2-zRtqHWdSWRi41TP3AZv86vODzJoCwnu0-UVVrTO1KH9BTkGOxTA1VkBES67K57a-Wgqbe200n3UhDp2_7D-_EQFU
Moran, D., Piacentini, L. and Pallot, J. (2016), 'Liminal Transcarceral Space: Prison Transportation for Women in the Russian Federation', in N. Gill, ed., *Carceral Spaces: Mobility and Agency in Imprisonment and Migrant Detention*, 109–24. Routledge.
Naples, N. and Gurr, B. (2014), Feminist empiricism and standpoint theory: Approaches to understanding the social world, in S. N. Hesse-Biber, ed., *Feminist Research Practice: A Primer* (2nd edn), 14–41. Thousand Oaks, CA: SAGE.
Nettler, G. (1974), 'Embezzlement Without Problems', *The British Journal of Criminology*, 14: 70–7. https://doi.org/10.1093/oxfordjournals.bjc.a046512
Noble, C. H. and Walker, B. A., (1997), Exploring the relationships among liminal transitions, symbolic consumption, and the extended self. *Psychology & Marketing*, 14: 29–47.
ONS. (2022), 'Homeworking and Spending During the Coronavirus (COVID-19) Pandemic, Great Britain: April 2020 to January 2022', available online at https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/homeworkingandspendingduringthecoronaviruscovid19pandemicgreatbritain/april2020tojanuary2022
Qian, J., Mills, M., Ma, H. and Turvey, S. T. (2022), 'Assessing the Effectiveness of Public Awareness-Raising Initiatives for the Hainan Gibbon *Nomascus hainanus*', *Oryx*, 56: 249–59.

Ramamoorti, S. (2008), 'The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula', *Issues in Accounting Education*, 23: 521–33. https://doi.org/10.2308/iace.2008.23.4.521.
Ramamoorti, S., Morrison, D. and Koletar, J. ,W. (2009), 'Bringing Freud to Fraud: Understanding the State-of-Mind of the C-Level Suite/White Collar Offender Through "A-B-C" Analysis', *Institute for Fraud Prevention (IFP) at West Virginia University*, 1: 1.
Raval, V. (2018), 'A Disposition-Based Fraud Model: Theoretical Integration and Research Agenda', *Journal of Business Ethics*, 150: 741–63. https://doi.org/10.1007/s10551-016-3199-2
Saluja, S., Aggarwal, A. and Mittal, A. (2022), 'Understanding the fraud theories and advancing with integrity model', *Journal of Financial Crime*, 29: 1318–28.
Sampson, R., Eck, J. and Dunham, J. (2010), 'Super Controllers and Crime Prevention: A Routine Activity Explanation of Crime Prevention Success and Failure', *Security Journal*, 23: 37–51.
Schuchter, A. and Levi, M. (2016), 'The Fraud Triangle Revisited', *Security Journal*, 29: 107–21. https://doi.org/10.1057/sj.2013.1
Seimetz, E., Kumar, S. and Mosler, H.-J. (2016), 'Effects of an Awareness Raising Campaign on Intention and Behavioural Determinants for Handwashing', *Health Education Research*, 31: 109–20. https://doi.org/10.1093/her/cyw002
Shields, R. (1991), *Places on the Margins: Alternative Geographies of Modernity*. London: SAGE.
Shortt, H. (2015), 'Liminality, Space and the Importance of "Transitory Dwelling Places" at Work', *Human Relations*, 68: 633–58. https://doi.org/10.1177/0018726714536938.
Smith, R. G. (2000), Fraud and financial abuse of older persons. *Current Issues in Criminal Justice*, 11: 273–91.
Smith, M. and Clarke, R. (2012), 'Situational Crime Prevention: Classifying Techniques Using "Good Enough" Theory, in B. Welsh and D. Farrington, *The Oxford Handbook of Crime Prevention*. Oxford, UK.
Stickle, B., Hicks, M., Stickle, A. and Hutchinson, Z. (2020), 'Porch Pirates: Examining Unattended Package Theft Through Crime Script Analysis', *Criminal Justice Studies*, 33: 79–95. https://doi.org/10.1080/1478601x.2019.1709780
Sutherland, E. H. (1940), 'White-Collar Criminality', *American Sociological Review*, 5: 1. https://doi.org/10.2307/2083937
Symantec. (2019), 'BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly', available online at www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019 (accessed 2 April 2021).
Trenerry, C. F. (2009), *The Origins and Early History of Insurance: Including the Contract of Bottomry*. New Jersey: The Lawbook Exchange.
Turner, J. E. (2012), 'Money Laundering Prevention', in J. E. Turner, ed., *Money Laundering Prevention*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119200604
Turner, V. (1974), *Dramas, Fields and Metaphors*. Ithaca, NY: Cornell University Press.
Van Gorp, B. and Vyncke, B. (2021), 'Deproblematization as an Enrichment of Framing Theory: Enhancing the Effectiveness of an Awareness-Raising Campaign on Child Poverty', *International Journal of Strategic Communication*, 15: 425–39. https://doi.org/10.1080/1553118x.2021.1988615
Vargas, C., Whelan, J., Brimblecombe, J. and Allender, S. (2022), 'Co-creation, Co-design and Co-production for Public Health: A Perspective on Definitions and Distinctions', *Public Health Research & Practice*, 32: 1–7.
Vedamanikam, M. and Chethiyar, S. (2020), Money mule recruitment among university students in Malaysia: awareness perspective'. *PUPIL: International Journal of Teaching, Education and Learning* 4: 19–37.
Vesty, S. (2022), 'Serial Romance Fraudster Splashed Victims' Cash at Scots Shopping Centre After Scamming £20k, Daily Record', 19 January 2022, available online at https://www.dailyrecord.co.uk/news/scottish-news/serial-romance-fraudster-splashed-victims-25990458?utm_source=linkCopy&utm_medium=social&utm_campaign=sharebar
Viollaz, J., Thompson, S. and Petrossian, G. (2021), 'When Human–Wildlife Conflict Turns Deadly: Comparing the Situational Factors That Drive Retaliatory Leopard Killings in South Africa', *Animals*, 11: 3281.
Vousinas, G. L. (2019), 'Advancing Theory of Fraud: The S.C.O.R.E. Model', *Journal of Financial Crime*, 26: 372–81. https://doi.org/10.1108/jfc-12-2017-0128
Warren, D. E. and Schweitzer, M. E. (2018), 'When Lying Does Not Pay: How Experts Detect Insurance Fraud', *Journal of Business Ethics*, 150: 711–26. https://doi.org/10.1007/s10551-016-3124-8
Webster, C. (2023), *Rich Crime, Poor Crime: Inequality and the Rule of Law*. Emerald Publishing Limited.
Wolfe, D. T. and Hermanson, D. R. (2004), 'The Fraud Diamond: Considering the Four Elements of Fraud: Certified Public Accountant', *The CPA Journal*, 74: 38–42.
Yar, M. (2013), *Cybercrime and Society*. London: Sage.