Original Research Article

JC

Conversations with deviant website developers: A case study of online shopping fraud enablers

Journal of Criminology
1–18
© The Author(s) 2025
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/26338076251321844
journals.sagepub.com/home/anj
Sage

Jack M Whittaker
Department of Sociology, University of Surrey, Stag Hill Campus, Guildford, United Kingdom

Michael R McGuire
Department of Sociology, University of Surrey, Stag Hill Campus, Guildford, United Kingdom

Suleman Lazarus
Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), London, United Kingdom; Department of Sociology, University of Surrey, Stag Hill, University Campus, Guildford, United Kingdom; Department of Sociology, University of the Western Cape, Cape Town, South Africa

Abstract

This study explores the experiences and challenges faced by Cameroonian website developers involved in creating non-delivery fraud websites. Through semi-structured interviews with 14 developers, four key themes were identified: (1) the psychological impact of the Ambazonian crisis, including heightened stress and anxiety due to ongoing civil conflict; (2) infrastructure disruptions, such as frequent power outages and Internet blackouts, which hinder their work and increase operational risks; (3) the influence of spiritual beliefs on decision-making, where concerns about offending ancestral spirits deter developers from direct fraud involvement; and (4) cultural perceptions of cybercrime, particularly the glorification of the "Big Boy" image, which normalises fraudulent activities as symbols of success. The study suggests that redirecting these developers' skills towards legitimate tech employment opportunities in Cameroon and internationally could help reduce cyber deviance and contribute to economic growth in affected regions.

Corresponding author:
Jack M Whittaker, Department of Sociology, University of Surrey, Stag Hill Campus, Guildford GU2 7XH, United Kingdom.
Email: j.m.whittaker@surrey.ac.uk

Keywords

Online fraud, pet scams, cyber deviance, non-delivery fraud, crime enablers, West African fraud

Date received: 29 September 2024; accepted: 4 February 2025

> Perfect as the wing of a bird may be, it will never enable the bird to fly if unsupported by the air.[1]
> (Pavlov, 1936)

Introduction

Fraud has traditionally been defined as the use of deception for personal gain. Typically, perpetrators will use false or misleading information to gain an unfair advantage over their intended victim (Beals et al., 2015; Edwards et al., 2024). The critical characteristics of deception are reasonably understood, centring upon factors such as the omission or distortion of information (Button & Cross, 2017). Less well understood are its relational aspects – how effectively a deceiver is able to persuade their victim that what they say or do is genuine or can be trusted. Even less understood are its mechanics the tools or techniques required for the deception to occur (McGuire & Holt, 2020). Or, as this is more commonly termed, what *enables* it (Frosch et al., 2007). The latter issue is related to the former – the mechanics of deception may impact how effective it is – but these two questions are not identical. To deceive someone over the telephone clearly requires a telephone for this to occur, though *how* the deceiver uses this device to persuade their victim that what they say is genuine is a further issue. Thus, whilst the telephone may certainly assist in making the deception more effective – for example, by removing standard detection methods like eye contact or facial expression – the tool is not synonymous with the technique.

The issue of how deception is enabled and its relationship with the methods used to persuade victims is now a central theme in contemporary fraud studies. The considerable influence of digital networks and factors such as the "anonymity" of online communication are usually cited as reasons for the growth in fraud prevalence (Edwards et al., 2024). Still, there is a risk that this will result in a blurring between the (distinct) questions of persuasion and enablement (Button & Cross, 2017; Lazarus, 2024). In this paper, we will focus directly on the latter question, using the example of online shopping fraud and, more specifically, non-delivery fraud as a focus for analysing the mechanics of fraud enablement. As we will see, there are some useful correlations between the way online shopping fraud occurs and its success in persuading victims. But there is also a range of more complex issues to consider in how online shopping frauds can occur, which have been overlooked in the simplistic formulation that the "Internet enables fraud." Our study points towards a more developed series of infrastructures behind online fraud, rooted in social and cultural factors and technical ones. These emphasise why there is a lot more to consider in evaluating how contemporary frauds occur than the techniques deployed by an immediate perpetrator using digital technologies. For fraud to be possible, there must usually be a range of supporting factors, which also come with their own characteristics and considerations. In particular, a proper understanding of the emergence and growth of fraud "online" is not only about the actions of perpetrators but also "active fraud enablers," which we define as "actors who actively assist an offender in the perpetration of their crime, with an intended result."

In this article, we will explore new data around a novel subculture of enablers, website developers in Anglophone Cameroon who knowingly build fake websites for offenders perpetrating online non-delivery frauds that target consumers in the "global north" (Whittaker & Button, 2020). We pay particular attention to the socio-cultural factors that have influenced them to engage in this type of work, and we consider what this might mean in terms of both understanding and preventing contemporary fraud in a more developed way. We begin by focusing on online shopping fraud, its key characteristics, and its prevalence. This, in turn, will be related to the anatomy of one particular type of non-delivery fraud, so-called "pet scams," that is particularly prevalent in the Anglophone region of Cameroon (Price & Edwards, 2020; Whittaker & Button, 2020).

Online shopping fraud

Over 2.14 billion people worldwide shopped online in 2021, a significant increase from 1.66 billion in 2016 (Statista.com, 2021). Secure transactions have supported this growth through public key encryption, enhanced digital payment systems, and multi-factor authentication. Additionally, the rise of major online retailers like eBay and Amazon and traditional retailers establishing online alternatives has contributed to this trend (Edwards et al., 2024). The COVID-19 pandemic further accelerated this shift, as many vulnerable populations, such as older people, could not shop in-store due to health risks.

The perceived benefits of online shopping have also driven its popularity. The convenience and cost savings of avoiding travel to physical stores (Rohm & Swaminathan, 2004) are compelling reasons for consumers to shop online. Additionally, online platforms allow consumers to search, compare, and access products and information more efficiently and in greater depth than traditional stores (Edwards et al., 2024; Rohm & Swaminathan, 2004). Moreover, online retailers often offer lower prices due to reduced overhead costs compared to brick-and-mortar stores.

However, these benefits have a downside – a greater exposure to online fraud (Reisig & Holtfreter, 2013; Whittaker et al., 2022). The inability to inspect products before purchase and the lack of direct contact between buyer and seller (Van Wilsem, 2013) increase the risk of fraud compared to in-person transactions (Reep-van den Bergh & Junger, 2018). Fraudsters exploit this by creating profiles on popular retail platforms like eBay and Amazon or deploying fraudulent websites appearing in search engine results. Yar (2016) suggests that online shopping fraud often involves "the online sale of goods that may have been stolen, counterfeit, damaged, or otherwise misrepresented in terms of their quality or features – or simply never delivered to the paying customer." It can encompass all aspects of a transaction, including delivery, payment, return, and refund fraud (Lee, 2021). The Home Office Counting Rules define online shopping fraud as: "…attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site (Home Office, 2021, p. 41)". These definitions are simplistic compared to Beals et al.'s (2015) taxonomy of mass-marketing fraud, which classifies "consumer products and services fraud" into three sub-categories (Whittaker et al., 2022):

(a) *Worthless or non-existent products:* Misleading claims about products that are exaggerated, undervalued, or non-existent.

(b) *Worthless or non-existent services:* False promotions for services that are unnecessary, misrepresented, or not delivered.
(c) *Unauthorised billing:* Victims are charged for unordered products/services or billed higher than advertised.

Table 1 uses data from the Crime Survey for England and Wales to highlight the growth of online shopping fraud in the United Kingdom. In the year ending March 2024, retail fraud rose by 7% to approximately 883,000 incidents despite declines in other fraud categories (ONS, 2024).

This article focuses on non-existent products ordered from standalone websites, excluding counterfeiting, as it often involves willing buyers (Wall & Large, 2010). Beyond the mechanics of online shopping fraud, understanding the network of enablers is equally vital.

Enablers and the infrastructure of contemporary fraud

The growth of contemporary fraud cannot be attributed solely to the significant expansion of e-commerce and online shopping nor to the associated technical and social factors. While these developments have certainly created new opportunities for individuals with the intention and capacity to exploit them, other, less-researched conditions have also played a crucial role. Levi (2022), Lazarus (2024), and Wang et al. (2021) highlight how enablers can operate within legal boundaries while facilitating illegal activities. Similarly, website developers who build and maintain fraudulent sites in online shopping fraud serve as pivotal, yet legally ambiguous, enablers. This legal ambiguity strengthens the resilience and expansion of fraudulent infrastructures, despite these activities being under-researched and difficult to regulate.

Scholars reveal a discernible divide within cybercriminal operations. For example, Levi (2022), Lazarus (2024), and Wang et al. (2021) distinguish between individuals who consciously facilitate criminal activities and those who, often inadvertently, become unwitting enablers, contributing to cybercrime without full awareness. Professionals such as lawyers, bankers, and accountants may choose to turn a blind eye to the presence of cybercrime enterprises rather than report them, thereby acting as passive agents in the cybercriminal landscape (Lazarus, 2024; Levi, 2022; Wang et al., 2021). For instance, accountants who, while conducting business on behalf of a cybercriminal entity, deliberately overlook its nefarious activities

Table 1. Crime survey for England & Wales data on fraud victimisation (2023–2024).

Offence group	April 2022–March 2023 Number of incidents (1,000)	April 2023–March 2024 Number of incidents (1,000)	Number of incidents % change
All fraud	3,526	3,177	−10
Bank and credit account fraud	2,135	1,885	−12
Consumer and retail fraud	825	883	+7
Advance fee fraud	391	302	−23
Other fraud	175	106	−39

effectively condone cybercrime (Lazarus, 2024). In the more specific context of the cybercrime economy, Leukfeldt and Holt (2019), Romagna and Leukfeldt (2023), and Leukfeldt et al. (2016) explore the social organisation of cybercriminals and enablers. Crucially, Leukfeldt and Holt (2019) identify that organised offenders recruit peer groups to complete offences and enable offending by providing the necessary equipment and support for their activities.

Frosch et al. (2007) provide a useful set of scenarios which tested how offenders and enablers are often viewed differently in terms of their respective culpabilities. Take, for example, the hypothetical case of Mary, who throws a dying cigarette into a bush. Another woman, Laura, then deliberately pours petrol onto it, which causes a nearby house to burn down. In this scenario, Mary enabled the fire whilst Laura caused it. When compared to enablers, respondents in the study tended to judge perpetrators as being more responsible for an act, liable for longer prison sentences, and liable to pay larger damages. Thus, in this scenario, Mary was certainly negligent in not putting out the cigarette first. However, since she was only a (passive) enabler for the resulting conflagration and did not intend for the house to burn down, Mary was judged as less culpable than Laura.

Recognising the role of these enablers is crucial for developing targeted interventions, as their actions, whether deliberate or unwitting, create opportunities for cybercriminals to exploit. To effectively address such complexities, Hutchings and Holt (2015) propose using crime script analysis to uncover the detailed interactions and roles within cybercrime markets. This method helps reveal the specific actions and interactions of various actors, such as website developers in online shopping fraud and provides insights into potential intervention points. The complexity of these interactions suggests that addressing online shopping fraud requires not only technical solutions but also a comprehensive understanding of the enablers and facilitators involved in these schemes.

While technical and social factors do play a role in enabling contemporary digital crime, the process of fraud has often been oversimplified within criminological theory. It is not merely "opportunity" that underpins the rise of contemporary fraud, nor is it sufficient to reference "the Internet" as a catch-all explanation for the underlying mechanics. Instead, a far more complex background enabling factors must be explored. One such factor is how fraudulent websites are generated and maintained. Fraudsters rely heavily on these websites to conduct their activities. Yet, there is limited understanding of the professional cadre of enablers who facilitate this process – the individuals who perform the groundwork of building these sites. How they do this, under what conditions, and how fraudsters leverage their skills are topics that are only beginning to be understood.

To illustrate some of these mechanics, we will examine a specific yet under-researched type of shopping fraud: the pet scam. By analysing how pet scam websites are created, broader insights into the mechanisms of fraud enablement can be gained. This approach not only highlights the technical and organisational aspects of such scams but also sheds light on the socio-economic and professional networks that underpin them, providing a more comprehensive understanding of fraud enablement.

However, before we look at the anatomy of a pet scam as a precursor to the analysis, it is important to consider that in this paper, we are looking at only one type of enabler, the deviant website developer, and that it is important to acknowledge that there are other types of enablers which this paper does not consider yet are worthy of future research. The deviant website developer's role is to enable this type of fraud by creating fraudulent websites on behalf of their fraudster clients and to ensure that these websites look like legitimate retail websites. A common technique used in the production of fraudulent websites is by downloading an entire legitimate website and then reuploading it online with the contact details (e.g., phone number and email address) of their fraudster clients. They may also create fraudulent websites by using text and images stolen from several legitimate donor websites.

In addition, these website developers need to source infrastructure providers who may also be enabling the fraud. This might be by using the services of a hosting provider that tolerates this type of activity (commonly known as "bulletproof hosts"). They also need to use the services of a domain name registrar, a company that sells the domain names. The Internet Corporation regulates domain name registrars for Assigned Names and Numbers ("ICANN"). However, cybercriminals are known to utilise the services of certain domain name registrars that are not likely to take fraudulent domains offline.

Lastly, this type of fraud is enabled by so-called "money mules," who specialise in setting up bank accounts in the target country of the fraud to repatriate the stolen funds back home. This might be by exploiting the services of "unknowing money mules," victims of romance fraud or victims of fraudulent part-time work opportunities (Leukfeldt & Kleemans, 2019; Raza et al., 2020). Money laundering may also take place through the use of complicit actors, "knowing money mules," who are often Cameroonian nationals that operate in the target country and sell their services to fraudsters with whom they are acquainted back in Cameroon (Leukfeldt & Kleemans, 2019; Raza et al., 2020).

Pet scams

Between 2020 and 2023, the number of scam-related websites rose from around 15,000 to more than 1.6 million (Statista, 2024). These include phishing sites, charity scams, fake shopping sites, or counterfeit ticket sales. Whilst the form and content of fraudulent websites may vary, their aims are usually similar – to obtain personal information or financial benefits from their victims. The websites used for pet scams conform closely to these characteristics. However, they usually aspire to be as visually appealing as possible to enhance the emotions of the animals they purport to sell. One especially interesting characteristic is their geography, which is usually centred upon a specialised manufacturing base situated in West Africa, especially in the Anglophone northwest and southeast regions of Cameroon (Better Business Bureau, 2017; Fuh, 2021; Price & Edwards, 2020; Whittaker & Button, 2020). Such websites are part of the broader industrialisation of fraud within this region and provide useful insights into the mechanics of fraud enablement there. Online pet scams rely on legitimate-looking websites and enticingly low prices to attract victims. The buyer's psychology often influences victimisation, including negative life events (Whittaker & Button, 2020). For instance, one victim, Karen, reached out to a fraudulent site after losing both her husband and her pet, highlighting how emotional vulnerabilities can drive decision-making as follows:

> My husband AND dog died last month, and I have been excited about adopting a pair of kittens because my home is pretty lonely now. (Karen)

Once a victim identifies an animal to purchase, they typically send an enquiry to the website, providing their phone number and email address. Offenders then communicate with victims via email, phone, text, or WhatsApp. Initial contact is used to groom the victim into trusting the offender and ultimately making a payment, as discussed in the literature on online romance fraud and related crimes (Bilz et al., 2023; Lazarus, Whittaker, et al., 2023). Offenders usually respond with pre-scripted messages containing fictitious details about the animal, promises of after-sale documentation, and pet care items to reassure the victim of the transaction's legitimacy. Rapport-building, often involving religious assurances, is a common tactic to gain trust before the victim makes an advance fee deposit. This is illustrated by Mili's case, where she received a religious justification for reassurance.

> We're a God-fearing Christian family and cheating people of their hard-earned money is not of our faith. (Mili)

After the trust-building process is undertaken, victims are subsequently pressured into making the advance fee deposit for their desired animal. The most common excuse used by offenders here is to ensure "same-day delivery," despite in some cases this being impossible because of the purported distance between the buyer and seller.

> Told me they can ship the pup same day and guarantee delivery to my door within 5–7 hours. Shipping from Minnesota to Ohio in 7 hours is amazing … amazingly false. (Karen)

Once the advance fee is paid for their desired animal, victims are contacted by the offender posing as a shipping company, demanding additional payments to cover transport and other costs. This technique, known in fraud literature as a "recovery scam," involves revictimising individuals using methods different from the original fraud (Titus et al., 2001, p. 135). The most common fee at this stage is a supposedly refundable charge for a "temperature-controlled shipping crate" to maintain the animal's body temperature and resist "harsh conditions" during transit (Whittaker & Button, 2020). These secondary fees typically exceed legitimate shipping costs by about 55% (Mehmedov, 2021). A possible explanation for why offenders charge a premium for shipping is that victims are stuck in a "sunk-cost fallacy," already invested to the extent that they are willing to continue participating in the fraud even if they are cognitively aware that the likelihood of receiving any value from the transaction has decreased (Chang & Chong, 2010). In addition to the cost of the shipping crate, fees introduced during this stage include veterinary and quarantine fees, registration documentation fees, and insurance fees (Whittaker & Button, 2020).

Methodology

This study utilised qualitative interviews with 14 Cameroonian website developers involved in creating non-delivery fraud websites. Access to participants was facilitated by a website developer from Bamenda, located in the Anglophone region of Cameroon, who acted as a gatekeeper. As an "introducer," he leveraged his extensive social network to bridge the relational distance between the researcher and potential interviewees. This approach, as defined by Jacques and Wright (2008, p. 2), helps reduce the "nature and degree of intimacy between recruiter, interviewee, and researcher," which can be influenced by factors such as the frequency and length of interactions and the strength of social ties (Black, 1976).

A key consideration was whether to conduct the research in person or virtually. Although in-person fieldwork might have facilitated trust-building with interviewees, an initial risk assessment highlighted significant safety concerns. The volatile security situation in the Anglophone region, marked by ongoing conflict between Anglophone separatists and the Francophone government, posed substantial risks. The United Kingdom Foreign, Commonwealth & Development Office advises against all travel to this area due to sporadic conflict and frequent kidnappings (Human Rights Watch, 2022). Additionally, the interviewer's visible foreign status could have attracted unwanted attention. Consequently, the research team adopted a desk-based approach, conducting interviews remotely via videoconferencing.

Data collection comprised an initial questionnaire followed by semi-structured interviews conducted through Zoom. The 28-question questionnaire gathered data on participant demographics, business operations, trust maintenance, experiences with website shut-downs, and associated impacts and concerns. Responses were then utilised as prompts during the semi-structured interviews, aligning with Braun and Clarke's (2006) approach to thematic analysis, which facilitates the identification and production of themes from participants' detailed accounts. Interview transcripts were shared with participants for review and validation. To protect participant confidentiality, pseudonyms were used, and identifiable information was removed. Informed consent was obtained from all participants, and no one was excluded based on predefined criteria. Fourteen participants (13 male and one female) completed both stages of the study. The research received ethical approval from the author's institution under reference number FASS 21-22 077 EGA.

Data analysis

Once the data had been collected, the interview transcripts were reviewed and subjected to a rigorous three-round coding process. The first round involved open coding, generating descriptive labels based on initial data observations. The second round, focused coding, identified patterns and relationships between the initial codes. The final stage of thematic refinement grouped codes into sub-themes and overarching themes. Both semantic and latent relationships between codes were explored to ensure a comprehensive and nuanced understanding of participants' experiences (Braun & Clarke, 2006).

Coding was conducted manually, enabling the systematic organisation, retrieval, and comparison of data through a hands-on, iterative process. The analysis process was grounded in collaborative efforts, with two research team members reviewing and refining preliminary themes to ensure reliability and rigour. Discrepancies in coding interpretations were resolved through iterative discussions, fostering a shared understanding of the data. Reflexivity was integral to the process: the research team, comprising individuals from diverse socio-cultural backgrounds, engaged in ongoing reflection to critically examine how their diverse assumptions and lived realities might shape their interpretations. Specific discussions, such as the role of spiritual beliefs in participants' decision-making, were undertaken to ensure interpretations were grounded in the data while acknowledging the inherently subjective nature of qualitative analysis and the researchers' interpretive lenses. Each theme was systematically evaluated for prevalence, with participant contributions carefully documented to assess significance in line with qualitative research best practices. The "psychological impact of the Ambazonian crisis" and "infrastructure disruptions" themes were highlighted by 11 participants each.

"Spiritual beliefs in decision-making" were mentioned by eight participants, while "Perceptions of Fraudsters and 'Big Boy Culture'" were identified by seven participants.

Participants were invited to review their transcripts and provide feedback to enhance authenticity. However, all participants declined, citing time constraints and expressing trust in the interviewer to accurately represent their narratives. A thematic map was developed during the analysis, initially identifying eight candidate themes. After a detailed review, three themes were reassigned as sub-themes due to their explanatory relationship with broader themes. One candidate theme was excluded for insufficient supporting data, in line with established qualitative research principles. The final thematic structure comprised four overarching themes and 12 sub-themes, representing key dimensions of participants' experiences listed above. These themes provide the foundation for the analysis presented in the subsequent sections.

Findings and discussion

The data analysis produced four themes: (1) the Amazonian crisis and psychological challenges, (2) disorder and infrastructure sabotage, (3) the role of spiritualism in decision-making, and (4) perceptions of fraudsters and "Big Boy Culture". These themes highlight the various influences faced by deviant website developers.

The Ambazonian crisis and psychological challenges

A central theme that we produced across all of the interviews, except for one (Timothy) who had moved out of the region, was the impact that the so-called "Ambazonian Crisis[2]" conflict has had on the website developer's ability to perform more complex work tasks for legitimate clients. As a useful contextual background to understanding the crisis, it is important to first note that Cameroon is a majority francophone country that comprises approximately 28.6 million people (Unfpa.com, 2024). There is, however, also a sizeable Anglophone community – approximately 17% of the country's population (Bang & Balgah, 2022) – concentrated in the northwest and southwest regions that border Nigeria. Of particular relevance to the findings of this article are the ongoing troubles in the Anglophone region, which started as peaceful demonstrations in 2016 when trade unionists and lawyers protested against the obligatory use of the French language in schools and Law courts (Bang & Balgah, 2022). Since 2017, these protests became violent when armed separatist groups emerged from within the Anglophone regions to engage in fierce sporadic conflict with government forces (Lazar, 2019). Separatists called for the secession of the two Anglophone regions, which they have labelled collectively as "Ambazonia" (Beseng et al., 2023; Human Rights Watch, 2022; Lazar, 2019). The ensuing conflict has resulted in atrocities being committed by both separatist and government forces. A report by Human Rights Watch published in 2022 estimated that the violence had resulted in approximately 6,000 civilian deaths, the displacement of 600,000 people internally within Cameroon, and over 77,000 Anglophones that had crossed the border to Nigeria as refugees (Human Rights Watch, 2022).

One of the interviewees, Azem, provided useful insight into the psychological challenges arising from the conflict in his account. He related how the fighting between separatists and Cameroonian government forces was undermining his ability to focus on more complex programming because he had to lie down in his house to avoid being hit.[3] Azem also described how clients from outside of the region were being "scared away" by the violence, further impacting upon his legitimate business opportunities.

> Oh my god, that's just the worst. That's just the worst. The crisis itself you just hear the gunshots on a daily basis. You cannot concentrate to do any work, like hard work for legit clients that requires actual coding, with the sound of gunshots in your ears. It's impossible. At times we really fear for our lives. Maybe you can go somewhere to meet a client from outside of town and you hear gunshots and everybody is suddenly running for their lives. Then the client doesn't return because of the risk and cuts off contact with me. Something like that. Even when you are home. Yesterday was Easter and so much gunshots the whole afternoon. I wanted to work but I couldn't because I was lying down in my room all day in case of being hit. When I went out the next day, I saw that my neighbour's property had been hit in four places. How can I be expected to concentrate on my work when I fear for my life? (Azem)

Another interviewee, Aziz, echoed similar sentiments, describing the challenges he faced while attempting to work amidst intense gunfights between separatist forces and the Cameroonian military in his compound. Aziz highlighted the detrimental effects on his mental well-being and his ability to focus on tasks for legitimate clients, stating:

> …sometimes if there's a gunfight between the government and the separatists you can't go out. You don't even sit down. You are in your house but you are on the floor. You have to actually sleep on the floor because you don't want a stray bullet hitting you. (Aziz)

Disorder and infrastructure sabotage

In addition to the negative psychological impacts of the armed conflict on their ability to concentrate and work, several interviewees also complained about acts of sabotage that are regularly committed against the local infrastructure and economy of the region by separatist forces aiming to damage the Cameroonian economy and by the Cameroonian government as reprisals. An ongoing problem discussed by the interviewees was the impact of so-called "ghost towns" on their ability to do work, an issue that has been recurring weekly since 2016 (Foute, 2024). The term ghost-town refers to the recurring shut-downs of social and economic life on certain days when separatist forces force residents to remain in their homes. The ghost town problem is, in principle, manageable because many interviewees reported working from home. However, power outages arising from sabotage attempts against the local electricity infrastructure made by separatist forces are far more problematic. So, too, are the routine issues with the electricity infrastructure, which cannot be rectified because employees of the electricity company supplying the region are unable to attend work to perform maintenance or repair damage. Aziz described that on ghost town days, he was often unable to do work for his legitimate client, a government institution, because the electricity outages prevented him from accessing his working device or the Internet. According to Aziz:

> I work with a government institution sometimes and on that Monday I don't work except if I'm being called up to complete a task from home. But there is one thing, Internet connection. During days of crisis, maybe the routers, our antennas, the service providers, they will come offline so you may not have lights, you may not have network. So it's kind of a

> problem where you might find that I am home on ghost town days and I don't do hard work for legit clients because I don't have Internet connection or I don't even have electricity. (Aziz)

As a result of the impact of their work of power failures on ghost town days, some of the interviewees attempted to find ways to generate their own electricity. The most common work-around described was to purchase an electricity generator. However, as Smith describes in the quote below, the expense of running electricity generators raises its own challenges. Generators require the use of petrol or diesel to function, meaning that they can only be run for a limited time – barely enough to charge their devices. Smith also pointed out that the generators offer only limited support because Internet access to the region is also unavailable during the power cuts. Smith stated:

> All of this is due to the crisis, because maybe if there is an electricity port somewhere but because yesterday was a ghost town and today is a ghost town maybe the people of the electricity company have not been able to rectify the problems because of the ghost town. So, it's actually affecting us so maybe I have not been able to sit on my computer now for like 2 hours straight because I only have to work with a generator and you cannot get fluids or petrol to fuel it the whole day. Maybe you can get some just to manage and charge your phones and get online and be updated and that's all. So, it's really difficult working in this kind of environment. No constant electricity, outages, network problems, there are days when we go without networks. It's really a big problem. (Smith)

The role of spiritualism in decision-making

The interviews revealed the profound influence of spiritual beliefs on decision-making among website developers in Cameroon. While the ongoing Ambazonian crisis may influence motivations differently, spiritual convictions emerged as a significant deterrent, steering developers away from direct involvement in online fraud. Instead, they focused on creating fraudulent websites. Interviewees frequently cited a reluctance to offend ancestral spirits as a primary reason for abstaining from direct fraudulent activities. This inclination towards ethical restraint reflects the "Traditional African Spiritual Systems" discussed by Lazarus (2019, pp. 1–18), where spiritual considerations play a pivotal role in shaping criminal behaviour. Lazarus (2019, p. 6) explores the notion of "escapelessness," prevalent in the broader West African context:

> Escapelessness meant that the ancestral spirits were thought to be all-knowing; no violation of the norms of society escaped their surveillance, and no offender did. The severity of sanctions was used to deter the rest of society; the ancestral spirits were thereby upholders of the socio-moral order.

Spiritual repercussions, therefore, act as powerful deterrents against transgressions, with ancestral spirits perceived as omniscient guardians of societal order, actively discouraging illicit activities and upholding moral standards (Assimeng, 1986; Lazarus, 2019). This traditional worldview, embedded in the Traditional African Spiritual Systems, continues to wield significant influence in contemporary West Africa (Lazarus, 2019, pp. 5–7), highlighting that self-regulation relies heavily on adhering to social norms and upholding legitimacy (cf. Tyler, 1990).

However, spiritualism's impact on these developers' actions and self-concept is nuanced. For some, spiritual beliefs foster a strong moral compass that guides their behaviour, deterring them from engaging in activities they perceive as directly harmful. This is evident in the way they rationalise their focus on creating fraudulent websites, which they view as a lesser offence compared to directly perpetrating fraud. For others, spiritualism functions more as a cultural backdrop, influencing their perception of what constitutes acceptable behaviour within their community. This explains why they may still engage in some forms of offending (enablement) that they deem less severe, thereby reconciling their actions with their spiritual beliefs.

For instance, Powoh narrated the prevalence of "black magic" rituals in Anglophone Cameroon, describing how participants might be required to adhere to specific prohibitions, such as "never wearing sneakers" or making solemn pledges like "giving up your father's life." According to Powoh, failing to honour these obligations could result in dire consequences, as he emphasised, "then it's your life that will go." Powoh's belief that such rituals contribute to the premature demise of many scammers led him to abstain from direct online fraud, noting that "most of the time you see them [scammers] dying at the age of 20–30 years old." This fear of spiritual retribution significantly influenced his actions and self-concept, reinforcing his decision to avoid direct fraudulent activities.

Conversely, two interviewees expressed scepticism towards these practices, dismissing them as "rubbish" and attributing the involvement of scammers in the region to their gullibility and susceptibility to manipulation. Jong, one of the interviewees, highlighted the negative impact of Ghanaian and Nigerian movies about black magic on the local mindset, referring to them as "poison" that distorts perceptions. He also refuted the existence of black magic ceremonies based on his personal experiences, stating that despite being in close proximity to actual fraudsters, he had never encountered such rituals. Jong contended that the proliferation of these movies in Cameroon fosters unfounded rumours, exaggerated claims, and illogical conclusions within the community. He argued that attributing success or failure to black magic rituals instead of rational explanations perpetuates misunderstanding and prejudice.

Jong further suggested that the adherence to black magic beliefs is shrouded in secrecy, likening it to a code of silence, a kind of omerta, enforced by priests. He questioned the validity of accusations of witchcraft within the community, suggesting that identifying individuals who subscribe to such ideologies is virtually impossible. According to Jong, the fraudsters involved in these practices are easily manipulated due to their exposure to misleading movie portrayals, falling victim to exploitation by local practitioners of black magic. As he noted:

> People believe a lot of the things they see on the Internet or in movies these days. So, it's just easy to manipulate people, and if the scammer is manipulating his victim into sending money through flashy websites, then it's almost certain that there is a juju priest manipulating a scammer by promising them riches under certain conditions. (Jong)

While spiritual beliefs serve as deterrents for some developers, they have little to no impact on others who view these practices as mere superstition. This dichotomy highlights the complex interplay between cultural beliefs, personal convictions, and criminal behaviour, underscoring the need for a deeper understanding of how these factors influence decision-making among website developers in this region. To fully grasp the impact of spiritualism on the self-concept and actions of these developers, future research should explore how these beliefs intersect with other socio-economic and cultural factors in shaping their involvement in fraud.

Perceptions of fraudsters and "Big Boy Culture"

The fourth theme discussed in this article is how the website developers perceived fraudsters in the local community, with several interviewees describing their lifestyle as "unattractive" because they were seen as problematic or immoral. While some interviewees (e.g., Asang and Emile) described how fraudsters in Bamenda were often viewed as "successful" by the local community, they were less persuaded because of certain activities and lifestyles on the part of fraudsters, which they viewed as troublesome. How fraudsters flaunted their wealth in the local community was viewed especially negatively. One of the interviewees, Vanesa, referred to "impression spending" as being an integral part of a "Big Boy" [fraud] culture because "everybody wants to chill with the big boys and have a seat there." Likewise, Powoh described how those fraudsters "want to be seen as superstars" in the local community, requiring them to spend money to satisfy this public image. Several of the interviewees were openly critical of the way fraudsters openly flaunt their wealth.

The negative perceptions of online fraudsters and the glamourisation of their wealth diverge from the established body of research on the social legitimacy of online fraudsters in West Africa, particularly in Nigeria and Ghana (Abubakari & Blaszczyk, 2023; Lazarus, Olaigbe, et al., 2023). This discrepancy is most evident in the tendency of many Afrobeats artists to glorify online fraudsters in their lyrics, thereby reinforcing their social legitimacy, as indicated by emerging qualitative studies (Lazarus, 2018; Lazarus, Olaigbe, et al., 2023). The influence of Afrobeats in shaping public perception highlights the significant role of popular culture in normalising cybercriminal activities, especially in Nigeria, Ghana, and Anglophone Cameroon, as well as among the African diaspora. Despite the pervasive influence of Afrobeats, the negative perception of fraudsters who flaunt their ill-gotten wealth remains a subject deserving further investigation.

Emile described how fraudsters in Bamenda have been purchasing "new clothes and trainers," "sports cars," and "power bikes," while Brando noted that they often invest in iPhones, stating, "they like to use the new version." These high levels of spending on luxury products elicited two different reactions from website developers. Ndifor expressed moral outrage, stating that fraudsters are "lying to themselves." He explained that while they initially justify fraud as a means to escape poverty, it quickly turns into a pursuit of unnecessary luxury. He compared them to children, squandering their earnings instead of using the stolen funds responsibly. The fraudsters' shamelessness further compounded his outrage, as they often proudly display their flamboyant purchases and talk openly about them.

> …more is that they are so proud of it, so proud of it, like you see them talking about it in the public without no shame. Instead, they are very prideful of it. I'm like wow. (Ndifor)

Ndifor also pointed to a further concern, which overlapped with the interviewee, Marcel. This was their belief that extravagant spending might attract other young people into perpetrating fraud and away from legitimate employment opportunities. Marcel, for example, described how one of his employees had left his business a few months before the research interview because they felt they could earn more money by becoming a fraudster. In his description of these events, Marcel noted that whilst his ex-employee had a new car, this made him "angry" because "the people will choose easy money over honest money."

These gendered dynamics in online offending provide additional context to the "Big Boy culture" discussed earlier. Over 92% of the website developers involved in creating non-delivery fraud websites interviewed are men. This finding is consistent with prior studies on online offending in West Africa. For example, Alhassan and Ridwan's (2023) interviews with online offenders in Ghana revealed that all participants (100%) were men. Similarly, Garba et al.'s (2024) analysis of convicted cryptocurrency fraudsters in Nigeria identified an exclusively male offender population. The dominance of men in this space reflects socio-cultural expectations that reinforce the "Big Boy" identity as an aspirational ideal. As Lazarus and Okolorie (2019, p. 23) note, "…men are more culturally expected to have economic power than women." In many West African societies, men are traditionally seen as primary providers for their families, including dependents such as wives, girlfriends, elderly relatives, and younger siblings. This pressure to fulfil provider roles is further intensified by the harsh economic realities many Cameroonians face, where limited opportunities for legitimate income generation may drive some men to offend online. The "Big Boy" lifestyle, characterised by extravagant spending and public displays of wealth, serves as both a driver and a symbol of success in this male-dominated space. These socio-cultural and economic pressures likely contribute significantly to the observed gender discrepancies in online deviance across the region.

Conclusion

This article has examined one process within the complex infrastructures of online fraud enablement, focusing on the accounts of website developers in the Anglophone region of Cameroon. The findings reveal that socio-political stressors, such as the Ambazonian crisis, combined with infrastructure sabotage and psychological vulnerabilities, significantly shape developers' decision-making processes. Fraudsters exploit these stressors, deepening the complexity of fraud enablement and highlighting the interplay of socio-economic and cultural factors with technical infrastructures. The findings underscore that the prevalence of contemporary fraud cannot be attributed solely to the Internet; rather, it is embedded within a broader socio-cultural and political framework that influences developers' actions and vulnerabilities.

This study advances the literature by demonstrating how fraud enablers operate at the intersection of structural constraints and individual agency. For instance, the findings align with Leukfeldt and Holt's (2019) work on the social organisation of cybercriminal networks, adding a nuanced understanding of how enablers like website developers function as pivotal intermediaries. Additionally, the study contributes to the growing research on gender dynamics in online deviance, where over 92% of the developers interviewed were male. This gender disparity reflects broader patterns in West Africa, as noted in prior studies (e.g., Alhassan & Ridwan, 2023; Garba et al., 2024), which highlight the cultural expectations of men as economic providers and their susceptibility to economic pressures that drive participation in cybercrime. By situating these findings within existing scholarship, this article offers a unique perspective on the socio-cultural underpinnings of fraud enablement in conflict-affected regions. A more nuanced solution to addressing online fraud is clearly required, one that better acknowledges the role of enablers and seeks to directly involve them in prevention efforts. Three primary policy recommendations emerge from this study.

First, programmes should be developed to harness the skills of website developers for legitimate employment opportunities, both in Cameroon and beyond. These programmes must address socio-economic and psychological barriers that prevent developers from transitioning to lawful work. For instance, vocational training programmes tailored to equip developers with skills in legitimate sectors, such as web development for non-profit organisations or private enterprises, could help redirect their expertise. However, implementing such initiatives requires overcoming infrastructural challenges in conflict-affected regions, such as limited access to stable Internet and electricity. Partnerships with international tech companies and NGOs could provide critical support by offering remote work opportunities, equipment, and funding.

Second, education-based interventions should be introduced to disrupt fraud further upstream, targeting website developers at local universities and institutions. These initiatives could challenge developers' justifications for working with fraudsters by fostering awareness of the emotional and psychological toll fraud takes on victims. For example, developers could be shown how fraud impacts vulnerable individuals, such as those seeking pets for emotional support during difficult life events. By humanising victims and dispelling myths, such as the belief that victims are "greedy," education could instil ethical responsibility among developers. Additionally, this approach should address the cultural and spiritual beliefs that shape developers' decisions. Fears of ancestral retribution and scepticism towards black magic rituals create unique barriers and justifications for fraud participation, as Lazarus (2019) noted. Tailored workshops that contextualise these beliefs within broader ethical frameworks could resonate more effectively with developers and promote ethical behaviour.

Finally, the role of university lecturers in shaping attitudes and behaviours should not be underestimated. Some lecturers perpetuate a culture of tolerance towards cybercrime by trivialising fraud in their classrooms (see Whittaker, 2024, p. 173). Sensitisation workshops for lecturers could emphasise their role as educators and role models, equipping them with strategies to proactively address cybercrime behaviours among students. These workshops should include training on identifying early signs of deviance and fostering a culture of accountability and ethical responsibility within academic institutions. Particular attention should be given to addressing cybercrime among male students, as over 92% of website developers interviewed in this study were male. This gendered focus aligns with broader findings in West Africa, where cultural pressures and limited economic opportunities disproportionately drive men towards online deviance. Future research should evaluate the efficacy of these interventions, particularly in regions affected by socio-political instability, to build a more comprehensive understanding of how to disrupt online fraud at its roots.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the University of Surrey Doctoral Studentship Fund (project code: TV8168).

ORCID iDs

Jack M Whittaker https://orcid.org/0000-0002-3669-9066
Suleman Lazarus https://orcid.org/0000-0003-1721-8519

Notes

1. See https://www.nature.com/articles/137572a0.
2. The "Ambazonia crisis" refers to the ongoing civil war between the Cameroonian government and English-speaking separatists in the Anglophone region.
3. The research team were informed after the conclusion of the interviews that one of the interviewees had been killed in crossfire between separatist and government forces.

References

Abubakari, Y., & Blaszczyk, M. (2023). Politicization of economic cybercrime: Perceptions among Ghanaian Facebook users. *Deviant Behavior*, *45*(4), 483–502. https://doi.org/10.1080/01639625.2023.2253487

Alhassan, A. R. K., & Ridwan, A. (2023). Identity expression – The case of "Sakawa" boys in Ghana. *Human Arenas*, *6*(1), 242–263. https://doi.org/10.1007/s42087-021-00227-w

Assimeng, M. (1986). *Social structure of Ghana*. Ghana Universities Press.

Bang, H. N., & Balgah, R. A. (2022). The ramification of Cameroon's Anglophone crisis: Conceptual analysis of a looming "Complex Disaster Emergency". *Journal of International Humanitarian Action*, *7*(1), 1–25. https://doi.org/10.1186/s41018-022-00114-1

Beals, M., DeLiema, M., & Deevy, M. (2015). *Framework for a taxonomy on fraud*. Stanford Center on Longevity.

Beseng, M., Crawford, G., & Annan, N. (2023). From "Anglophone problem" to "Anglophone conflict" in Cameroon: Assessing prospects for peace. *Africa Spectrum*, *58*(1), 89–105. https://doi.org/10.1177/00020397231155244

Better Business Bureau. (2017). Puppy scams: How fake online pet sellers steal from unsuspecting pet buyers. https://www.bbb.org/globalassets/article-library/puppy-scam-study/puppy-scams-bbb-study-20170901.pdf

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers*, *35*, 773–788. https://doi.org/10.1093/iwc/iwad048

Black, D. (1976). *The behavior of law*. Academic Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims* (1st ed.). Routledge.

Chang, J. J. S., & Chong, M. D. (2010). Psychological influences in e-mail fraud. *Journal of Financial Crime*, *17*(3), 337–350. https://doi.org/10.1108/13590791011056309

Edwards, M., Whittaker, J. M., Cross, C., & Button, M. (2024). An exploratory study of victimisation and near misses in online shopping fraud. *Global Crime*, *26*, 1–21. https://doi.org/10.1080/17440572.2024.2423918

Foute, F. (2024). Anglophone Cameroon: Buea near normal, while Bamenda a ghost town. https://www.theafricareport.com/31216/anglophone-cameroon-buea-near-normal-while-bamenda-a-ghost-town/

Frosch, C., Johnson-Laird, P., & Cowley, M. (2007, August 1–4). It's not my fault, your honour, I'm only the enabler [Paper presentation]. 29th Annual Conference of the Cognitive Science Society, Nashville, TN, United States.

Fuh, D. (2021). Chihuahua promises and the notorious economy of fake pets in Cameroon. *Journal of African Cultural Studies*, *33*(3), 387–403. https://doi.org/10.1080/13696815.2021.1949967

Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. *Current Issues in Criminal Justice*, 1–17. https://doi.org/10.1080/10345329.2024.2403294

Home Office (UK). (2021). *Fraud. Office counting rules for recorded crime* (p. 41). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/979916/count-fraud-apr-2021.pdf

Human Rights Watch. (2022). World Report 2022: Rights trends in Cameroon. https://www.hrw.org/world-report/2022/country-chapters/cameroon

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *The British Journal of Criminology*, *55*(3), 596–614. https://doi.org/10.1093/bjc/azu106

Jacques, S., & Wright, R. (2008). Intimacy with outlaws: The role of relational distance in recruiting, paying, and interviewing underworld research participants. *Journal of Research in Crime and Delinquency*, *45*(1), 22–38. https://doi.org/doi.org/10.1177/0022427807309439

Lazar, M. (2019). *Vol 283, Cameroon's linguistic divide deepens to rift on questions of democracy, trust, national identity. rep*. Afrobarometer.

Lazarus, S. (2018). Birds of a feather flock together: The Nigerian cyber fraudsters (yahoo boys) and hip hop artists. *Criminology, Criminal Justice, Law & Society*, *19*(2), 63–80.

Lazarus, S. (2019). Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions*, *10*(3), Article 146. https://doi.org/10.3390/rel10030146

Lazarus, S. (2024). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "black axe" confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023b). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology*, *2*, Article 100033. https://doi.org/10.1016/j.jeconc.2023.100033

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, *2*, Article 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Lee, C. S. (2021). How online fraud victims are targeted in China: A crime script analysis of Baidu Tieba C2C fraud. *Crime & Delinquency*, *68*(13–14), 2529–2553. https://doi.org/10.1177/00111287211029862

Leukfeldt, E. R., & Holt, T. J. (2019). Examining the social organization practices of cybercriminals in The Netherlands online and offline. *International Journal of Offender Therapy and Comparative Criminology*, *64*(5), 522–538. https://doi.org/10.1177/0306624(19895886

Leukfeldt, E., & Kleemans, E. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In S. Hufnagel, & A. Moiseienko (Eds.), *Criminal networks and law enforcement: Global perspectives on illegal enterprise (transnational criminal justice)* (1st ed., pp. 75–89). Routledge.

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2016). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Levi, M. (2022). Lawyers as money laundering enablers? An evolving and contentious relationship. *Global Crime*, *23*(2), 126–147. https://doi.org/10.1080/17440572.2022.2089122

McGuire, M., & Holt, T. J. (2020). *The Routledge handbook of technology, crime and justice*. Routledge.

Mehmedov, R. (2021). Automated classification of pet scam websites.

ONS. (2024). Nature of fraud and computer misuse in England and Wales: Appendix tables. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables

Price, B., & Edwards, M. (2020). Resource networks of pet scam websites. 2020 APWG Symposium on Electronic Crime Research (*e*Crime), 1–10. https://docs.apwg.org/ecrimeresearch/2020/71_Resource_Networks_Of_Pet_Scam_Websites.pdf

Raza, M. S., Zhan, Q., & Rubab, S. (2020). Role of money mules in money laundering and financial crimes a discussion through case studies. *Journal of Financial Crime*, *27*(3), 911–931. https://doi.org/10.1108/jfc-02-2020-0028

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, *7*(1), 1–15. https://doi.org/10.1186/s40163-018-0079-3

Reisig, M., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime*, *20*(3), 324–337. https://doi.org/10.1108/jfc-03-2013-0014

Rohm, A. J., & Swaminathan, V. (2004). A typology of online shoppers based on shopping motivations. *Journal of Business Research*, *57*(7), 748–757. https://doi.org/10.1016/s0148-2963(02)00351-x

Romagna, M., & Leukfeldt, R. E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, *47*(4), 511–529. https://doi.org/10.1080/0735648x.2023.2216189

Statista. (2021). Digital Buyers Worldwide 2021. https://www.statista.com/statistics/251666/number-of-digital-buyers-worldwide/#:~:text=Global%20number%20of%20digital%20buyers%202014%2D2021&text=In%202021%2C%20over%202.14%20billion,global%20digital%20buyers%20in%202016.&text=Purchasing%20goods%20and%20services%20online,many%20people%20around%20the%20world

Statista. (2024). Number of global phishing sites 2024. https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/

Titus, R., Groves, A., & Farrell, G. (2001). Personal fraud: The victims and the scams. In *Repeat victimization* (pp. 133–152). Criminal Justice Press.

Tyler, T. (1990). *Why people obey the law*. Yale University Press.

Unfpa.com. (2024). World population dashboard – Cameroon. https://www.unfpa.org/data/world-population/CM

Van Wilsem, J. (2013). "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. *European Sociological Review*, *29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Wall, D., & Large, J. (2010). Jailhouse frocks: Locating the public interest in policing counterfeit luxury fashion goods. *British Journal of Criminology*, *50*(6), 1094–1116. https://doi.org/10.1093/bjc/azq048

Wang, P., Su, M., & Wang, J. (2021). Organized crime in cyberspace: How traditional organized criminal groups exploit the online peer-to-peer lending market in China. *The British Journal of Criminology*, *61*(2), 303–324. https://doi.org/10.1093/bjc/azaa064

Whittaker, J. M. (2024). *Towards an understanding of enablement in online non-delivery fraud* [Doctoral dissertation]. University of Surrey. https://doi.org/10.15126/thesis.901339

Whittaker, J. M., & Button, M. (2020). Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. *Australian & New Zealand Journal of Criminology*, *53*(4), 497–514. https://doi.org/10.1177/0004865820957077

Whittaker, J. M., Edwards, M., Cross, C., & Button, M. (2022). "I have only checked after the event": Consumer approaches to safe online shopping. *Victims & Offenders*, *18*(7), 1259–1281. https://doi.org/10.1080/15564886.2022.2130486

Yar, M. (2016). *Oxford research encyclopedia of criminology*. https://doi.org/10.1093/acrefore/9780190264079.013.112