The British Journal of Criminology, 2022, **XX**, 1–18
https://doi.org/10.1093/bjc/azac098
Article

OXFORD

Confirm Not Command: Examining Fraudsters' Use of Language to Compel Victim Compliance in Their Own Exploitation

Elisabeth Carter*

*E. Carter, Kingston University, Department of Criminology, Politics and Sociology, Kingston University (London), Penrhyn Road, KT1 2EE, England; email: e.carter@kingston.ac.uk

Using discourse analysis to examine exchanges between fraudsters and victims in telephone-mediated frauds, this research examines the interactional techniques used by perpetrators of fraud to gain and maintain compliance from their victims, without causing them alarm. It reveals how compliance is secured and maintained in a process of establishing the relationship, grooming the victim and setting expectations of follow-through. Reimagining traditional understandings of fraud victimization and vulnerability, this work exposes how social and interactional norms are replicated and manipulated by fraudsters in order to compel individuals to be drawn into participating in an alternate, exploitative reality that is indistinguishable from safety; quashing a victim's ability to recognize the situation as harmful and rendering any motivation to escape as nonsensical. In doing so, this paper questions the efficacy of public fraud protection guidance strategies and delivers evidence for the need to change the present approach to understanding and tackling fraud victimization and complicity.

KEY WORDS: fraud, scams, interaction, compliance, fraud protection, public protection

INTRODUCTION

Unlike other acquisitive crimes such as burglary, where goods are taken without the victim's engagement, fraud is a crime where active participation from the victim is needed to directly facilitate the perpetrator's access to their money or data (Cross 2015). Indeed, with more than 99% of cybercrime threats requiring some level of interaction by the victim to succeed (Proofpoint 2019), and victim cooperation or facilitation 'often indispensable' (Titus 1999: 2), the expectation is that capable individuals should manage their own risks (Burchel 1996; Garland 1996), and adequate self-protection mechanisms (and their diligent application to everyday life) will reduce levels of fraud victimhood. Public-facing fraud protection and

awareness-raising information is built on this premise that effective fraud protection can be achieved through individual action. A key part of this is the narrative that individuals are able to identify fraudulent interactions and have the agency to take action to end them, or can adequately protect themselves from them through vigilance. Yet advice on this premise appears to fall short of its desired effect, with fraud the most commonly experienced crime in England and Wales (Crown Prosecution Service 2022), even though only 15% of victims report it (Crime Survey for England and Wales 2019). The increasing numbers of victims despite the continued low reporting rate, and increasing proliferation of fraud protection advice and awareness campaigns give rise to the question of how do fraudsters' criminal actions continue to succeed. This paper draws on a case study approach to explore how fraudsters in cases of telephone-mediated fraud convince victims to seemingly willingly comply with requests to perform acts that lead to their financial and psychological harm. It examines the reality of coercion during fraudulent interactions, and the implications of this reality in relation to current academic and practitioner understandings of this type of criminality, and practices in terms of protecting individuals from its harms.

LITERATURE REVIEW

Commonly, work in this area aims to understand vulnerability to victimhood through examining individual vulnerabilities in relation to different types of persuasive tactics (Langenderfer and Shimp 2001), susceptibility to fraud (Nguyen et al. 2021), and through examining victim accounts and recollections rather than empirical data of the crime itself (see Carter 2021 for an overview). Despite there being no significant correlation between individual differences and victimhood (Jones et al. 2019), examining what makes fraudulent communications so effective rather than what makes victims susceptible remains underexplored (Carter 2021; Kikerpill 2021). Recent work (Carter 2021) initiated a move away from understanding victimhood through traditional indicators of vulnerability, and, drawing parallels with domestic violence and abuse and coercive control, called for a shift towards viewing and understanding the power of persuasion in terms of the perpetrator's actions. The present research continues this trajectory; developing it by focussing on the social and interactional mechanisms exploited by fraudsters to compel individuals into becoming complicit in their own exploitation, and crucially, with their apparent consent and without causing them alarm. This is not to dismiss the relevance of individual situations in relation to vulnerability, and the power of circumstances such as loneliness (Buil-Gil and Zeng 2021) and social isolation (CIFAS 2020), or that specific circumstances are indeed leveraged and taken advantage of by perpetrators (Cross 2015), but instead to assert the need to also understand victimhood within the broader social and interactional frameworks that fraudsters exploit that makes all individuals susceptible to fraud, and not just those who are traditionally or legally recognized as 'vulnerable'.

Drawing on emotional and rational influences as tools of behavioural manipulation has been explored in various contexts, falling broadly within Cialdini's (2007) six categories of influence; reciprocity, commitment/consistency, social proof, liking, authority and scarcity. Convincing the victim of the legitimacy of the communication is important in compelling their compliance (Tzani-Pepelasi et al. 2020), with subservience to authority a way in which compliance is gained in relation to involvement in human rights abuses (Cohen 2001) and an individual's trust in the authority and legitimacy of the fraudster key to scam victimization (Button et al. 2009, 2014; Bidgoli and Grossklags 2017). Genre-mapping (Carter 2015) is an interactional mechanism through which fraudsters validate their communication by explicitly or implicitly matching legitimate communications, impersonating a genuine organization, by spoofing for example, or through harnessing the communication style of that organization or particular

sector respectively. This provides a 'legitimate guise' (ACTSO 2014) for fraudsters to enter into communications with a target and legitimizes direct threats within that context (Bidgoli and Grossklags 2017), mitigated through the contextual relevance of the communication, for example, in the early stages of the pandemic, by offering 'essential' or 'legally required' covid information or protections (Kikerpill and Siibak 2021)

Harnessing recognized contexts and current events makes misinformation appear more credible as it compels the recipient to make an emotional link which is laced with value judgement (Reyna 2021). Kircanski et al. (2018) found a link between emotionally arousing content and susceptibility in financial frauds, with Naksawat et al. (2016) finding the narrative in Nigerian 419 scams was specifically framed to elicit emotional responses. My own work in romance fraud shows how fraudsters invoke compliance through an emotional connection or sense of duty, a protective response drawn from the fraudster's use of visceral statements claiming some current or imminent psychological or physical harm (Carter 2021). Appealing to individuals' responses to values and emotion, rather than requiring victims to assess information on which to base their decisions, is particularly effective as they cannot be disprovable or discoverable as fraudulent. 'Gist representations' (Reyna 2021) resonate with internal narratives of individuals across a wide range of audiences and targets, much like cold psychic readings that rely on Barnum statements to induce feelings of individualized insights from generic statements (Roe 1996; Rowland 2002). Kikerpill and Siibak (2021) examine the interplay between tactics that involve the use of authority and the façade of benevolence; describing the carrot approach, where, in the 'Good Samaritan' approach, some need of the victim is (promised to be or appears to be) met; and in the stick approach, described as 'Shock and Awe', compels the victim to act in order to prevent some kind of loss. The present research examines how fraudulent interactions harness the social and interactional expectations that underpin legitimate interactions to obtain compliance from individuals where this will lead to their own financial and psychological harm, without causing alarm.

METHODOLOGY

This paper draws on empirical data in the form of recorded interactions between fraudsters and their victims, where fraudsters have contacted individuals by telephone in order to defraud them through remote access fraud and bank card fraud. The calls were recorded interactions due to the fraudster in each case telephoning an individual who had installed a TrueCall device and used the record function to save a record of the interaction. The subjects of the fraudulent calls gave the recordings to TrueCall (a company that works in the fraud protection sphere and provides free call-blocking systems to the public through local government authority schemes) with permission for them to be placed in the public domain. I was provided with 16 telephone interactions held by TrueCall. These interactions were not generated for the purpose of the research but were pre-existing data created as a result of the fraudulent interaction. The cases presented in this paper were selected as the longest calls and therefore provided the greatest opportunity to yield a range of interactional phenomena. All data was collected with ethical approval from the University and I transcribed and fully anonymized the audio interactions so that no identifying information remained; all transcripts used were also reviewed by the director of TrueCall to ensure accuracy and compliance with data sharing laws and principles. There is no conflict of interest in relation to the role of TrueCall and this research, as the relationship is entirely limited to their non-commercial provision of data for my research. There is no commercial interest of the company in relation to this research, analytic process or dissemination.

Drawing on spoken interactions the examination of the interaction-in-action that involves an interpersonal element absent from written communications, which makes it more effective in

terms of social engineering (Maggi 2010). The context provides the dynamic immediacy of the live 'performance' where rapid responses are interactionally encouraged through harnessing the problematization of delay in conversation (Fox Tree 2002), without revealing the true purpose of the contact. On a practical level, telephone interactions also represent the sole way in which spoken frauds-in-action can be captured and accessed for analysis.

This research uses a multiple case study approach to allow the 'investigat[ion of] a contemporary phenomenon, focusing on the dynamics of the case, within its real life context' (Teegavarapu et al. 2008: 4). As discussed in Carter (2021), the use of a case study approach is essential when examining frauds where the modus operandi is the development of rapport and trust over multiple interacting turns with the target victim. This approach aligns with the discourse analytic tradition of recognizing that individuals work together to create their social identities through interaction and is cognizant of the amount of data each interaction comprises (case 1: 2,641 words over 301 turns; case 2: 632 words over 72 turns; case 3: 917 words over 95 turns). A key characteristic of many types of fraudulent interactions is the extended length of the interaction, and a case study approach enables this work to represent and reflect fraudsters' establishment and development of interaction and rapport with victims, through which compliance is won and maintained, which is part of the reason frauds are so effective (Carter 2021). Critical discourse analysis, rooted as it is in the tradition of symbolic interactionism, is used to draw out and capture the nuance of the interaction while allowing space for the analysis of three different cases. Drawing on single extracts presented in a comparative fashion from a larger number of cases would obscure the interactional processes within each fraud that is the very focus of this work. The current work broadens understandings of fraudulent behaviours by delivering important insights into how language is used to deceive and exploit, reflected in the balance between depth of analysis and breadth of cases.

The combination of critical discourse analytic and pragmatic perspectives enables the inductive line-by-line examination of interactions to identify the fraudsters' use of lexis and orientations to contextually-relevant discursive practices and power relations that demonstrate and reinforce their (false) identities as official, credible, trustworthy interlocutors, and subsequently compel victims' continued engagement and compliance. The use of a pragmatic approach enabled the implicature embedded in the interaction to be drawn out in terms of the fraudster's talk and its meaning in context; the use of language to further this perlocutionary goal. For example, the conversational implicature of 'so'-prefaced turns situates that turn in a wider continuing conversation, thus compelling the victim to remain on the call. This work therefore draws on analytic frameworks that enable the exploration of both the communicative influence and persuasion of the interaction-in-action within the wider context of public protection.

The interactions examined in this research involve fraudsters vishing (voice phishing), also known as telephone-mediated fraud, in order to gain remote access to a victim's computer (case 1, extracts 1a–e) and bank card information (case 2, extracts 2a and b, case 3, 3a–c) in order to gain the details needed to defraud them. Each line of the extracts is numbered to reflect their relative position in the telephone interaction from which they are taken, and for ease of reference when discussing specific lines. The fraudster (F) is referred to as such throughout, as is the victim (V).

ANALYSIS

Case 1

The extracts that comprise case study 1 are transcribed from a case where a fraudster telephones the victim, claiming to be from a computer company, in order to draw the victim into unknowingly allowing him remote access to their computer, access which the fraudster can then abuse

for financial gain. The call is framed as a 'check up', and the opening extract (1a) shows the fraudster gaining the recipient's initial compliance with the call, in terms of staying on the line.

Extract 1a

1. F: Hi good morning to you sir you are talking to Mark and I'm calling you
2. from the IT department of S R Manning, and this call is about your computer.
3. Are you the main user of your computer sir?
4. V: Mmm
5. V: Yes- yes,
6. V: Hello?
7. F: Yeah can I speak to the main user of the computer sir?
8. V: It's me
9. F: Ah let me tell you Mr Newing, the reason of my call is just to make you
10. informed, now that whenever the computer user are going to online, some
11. programmes are getting automatically downloaded from internet. And due to
12. this many windows-based computers in London are getting affected. So
13. whenever the computer user are trying to go to online, trying to send a mail,
14. receive emails, do online banking, something, playing online games, at that
15. point of time. And due to this many windows based computers and laptops is
16. getting affected. Since you are one of the genuine user of the computer,
17. and we are the technical team that is the reason Mr Newing, you are
18. receiving this check-up call for your computer
19. V: Mhmm

After detailing his credentials, the fraudster opens the interaction with a series of statements beginning with 'you are', 'I'm', and 'this call is'; establishing the situation, the role of him as caller, and the purpose of the call. This continues in more detail in the fraudster's subsequent turn (lines 9-18), where he affirms his role as one of provider of important information, and the victim, as the 'main user of the computer' (lines 3 and 7) as the identified recipient of essential information and much-needed service. This further detail is framed using the word 'just', which minimizes the potential risk of accepting the proposed interference by limiting it to 'information only'. Further to this, the supply of information to the recipient is predicated on the authenticity of the *recipient's* status ('since you are one of the genuine user', line 16). This highlights the *dual and joint legitimacy* of both parties as a reason for the fraudster's phone call and for the offer, supported with the fraudster's 'and we are the technical team' (line 17); which situates his credibility as equal to the victim's; implicitly addressing potential concerns from the recipient by deflecting concerns of legitimacy away from the fraudster (Carter 2015).

Once this dynamic (in which the fraudster is at once an authority and an equal) has been established, the talk then quickly moves beyond 'just' making the victim informed. The use of 'so' on lines 10 and 12 is interesting as 'so'-prefaced statements are a discourse marker that indicate a link between statements and is important in constructing a narrative sequence across a speaker's turns (Johnson 2002). These enable the fraudster to link the situation he has outlined and the effect on other customers' (and by proxy the victim's) computers, without directly topicalizing it. This is then reinforced through the fraudster's 'and'-prefacing in the same turn ('And due to this', line 15); an interactional device that normalizes or makes routine an otherwise potentially concerning or unexpected turn, and 'warrant[s] a forward topical movement or shift in a possibly problematic environment' (Heritage and Sorjonen 1994: 21) through its link to a previous turn.

In his next turn, the fraudster uses 'so' again; leveraging the prior talk about an issue affecting computers to mitigate his dictating of the victim's physical movements ('get in front of the computer', line 20), check he has complied ('So are you in front of the computer' line 24), and require him to interact with his computer in the way specified by the fraudster ("now just have a look on your computer, line 26; 'so just give a single left click on the start [button]', line 35). Across the course of extracts 1a and, later, 2b, the fraudsters successfully shift the focus from 'just to make you informed' (lines 9 and 10) to initiating the process that will culminate in co-opting the victim into facilitating the fraudster's illegitimate and injurious access to his computer. This move from benign to more risky demands of the victim is mitigated through the fraudster's explicit pre-account ('for the sake of use', line 20), which delivers a practical reason for why the victim needs to comply with his directives, in addition to the use of both 'so-' and 'and-' prefaced turns, and the addition of 'just' on lines 26 and 35 downplaying the increasing risk to the victim.

Extract 1b

20. F: So Mr Newing for the sake of use, can you get in front of the computer, I am
21. holding the line for you ok. Just take your time,
22. V: Mhmm [computer sounds]
23. V: Yes,
24. F: So are you in front of the computer now sir?
25. V: Yes
26. F: So now just have a look on your computer now sir on the very extreme left
27. hand side bottom corner
28. V: Mhmm
29. F: Can you see there's a … like start button? There's a start button?

.
.
.

35. F: Ok. So just give a single left click on the start [button]

The fraudster's 'I am holding the line for you … take your time' (lines 20-21), although ostensibly telling the victim not to rush, performs the opposite as it positions the fraudster as waiting for the victim; the very topicalization of the (non) issue adds awareness of time pressure, forming an implicit urgency cue. It also diverts the victim's attention away from decision-making in relation to whether to perform the action or not, and on to the practicalities of completing the action.

The turns on these lines set up the scope of the interaction that follows; questions on the practicalities required in bridging the move between informing the victim to directly scripting their actions, such as ensuring the victim is in front of his computer (line 24), and locating the first button to press (lines 26 and 28). The victim then, under the fraudster's guidance, begins their navigation of the computer, the direct scripting of the victim's actions required for this ('give a … click on the start button', line 20) accounted for by the earlier 'for the sake of use' (line 20), linked back to this by the fraudster's use of 'so' (lines 24, 26).

Following this, and over several turns, the victim is then directed to locate and open the 'event viewer' on his computer, revealing multiple (benign) entries. In the following extract we pick up

the interaction at the point where the information in the event viewer is then erroneously used by the fraudster as evidence that harmful errors are present in the victim's computer at that very moment, and will increase: 'Right now … they will multiply each and every day into your operating system' (line 145). The fraudster then uses these (linked through the use of 'so', line 174), as evidence of a present (through the use of the present tense 'are harming', 'have', and 'already') and explicit threat to the computer ('infected a significant part of the computer', lines 181/2), that requires immediate action.

Extract 1c

174. F: So Mr Newing sir have you any idea what these warnings are? It's
175. part of the computer sir?
176. V: Errr no? I don't really know, no
177. F: Well let me tell you Mr Newing, the errors that are running in your
178. computer, that you can see in your computer are harming your
179. secure applications.
180. V: Mmm
181. F: Which have already activated in your system and have infected a
182. significant part of the computer

The fraudster's 'have you any idea' (line 174) gives the illusion of a question but performs a set up for the victim to concede a lack of knowledge and for the fraudster to then provide the answer. It reinforces the knowledge differential between the participants, setting up the next turn where the fraudster 'demonstrates' an expertize essential to the protection of the victim's assets. This allows a shift in power towards the fraudster as he now positions himself as an educator and instructor; maliciously using the benign and easily mistaken as harmful error messages (Microsoft.com 2022) to falsely claim there is evidence of a malevolent presence in his computer.

The fraudster opens his next turn with 'let me tell you' (line 177), an activity-prefacing narrative disguised as a request, which forecasts the talk-to-come (Kidwell and González Martínez 2010), identifying it as information the victim doesn't yet know but needs to know. This holds the floor for the fraudster to deliver this information and also frames the activity of this turn as information-giving; validating the content and reinforcing the fraudster's position as knowledgeable and the victim as in need of that knowledge.

The dissonance between 'secure applications' (line 179) and 'harming' (Line 178) highlights the seriousness of the situation and the challenge it presents to the victim's previously safe state online. This is then built on by the fraudster in the next extract, where the victim is made complicit in agreeing that the viruses have affected the normal running of his computer. The fraudster's 'You must have noticed' (line 187) forces a positive response from the victim as it is value-laden with the expectation that the victim will be aware of what is framed as an obvious situation.

Extract 1d

187. F: Ah Mr Newing due to this you must have noticed that sometimes you
188. are working in the computer that is running sometimes slow?
189. V: Mmmhm
190. F: Sorry?
191. V: Yeah I have, yeah,
192. F: And sometimes when- when you use your computer it's used to
193. pausing for a couple of seconds then start working?

194. V: Yeah
195. F: And when you are working your internet goes slow and your internet
196. is running slow?
197. V: Mmmmhm,
198. F: Sorry?
199. V: I have noticed that, yeah,
200. F: Because these are the problems, because of the error warning, let me
201. show you the problem. So what you need to do sir is just close all that
202. down and just come back to normal desktop ok?

The fraudster then delivers a series of 'and'-prefaced questions (lines 192-193, 195-196), relating to situations that would not be unusual for anyone with a computer to experience at some point. Avoiding absolutes through the use of 'sometimes', and vague, commonly-experienced events or 'gist representations' (Reyna 2021), the fraudster uses a technique reminiscent of Barnum statements (Roe 1996) to present these common issues as unique to the victim and to their current situation. The fraudster uses the likelihood the victim will agree he has experienced these situations, as evidence of the legitimacy of his claims of the presence of a virus on the machine. It's also used to evidence the need for further action and engagement 'because there are the problems … let me show you … what you need to do' (lines 200/201). The 'let me' of this turn mirrors the fraudster's earlier turn on line 177 ('let me tell you'), however here the fraudster uses it to forecast a demonstration ('let me show you') rather than the upcoming provision of information. However, it will transpire that this demonstration will be performed by the victim rather than the fraudster, with the 'show you' comprizing the fraudster telling the victim to navigate to specific areas of his computer, something that would ordinarily cause alarm.

The demands from the fraudster are disguised as a joint enterprise, with two-fold evidence for this further action; from the computer's event viewer log, which the victim helped to uncover, and from the victim's lived experience of his computer's non-optimal function. This demonstrates how the fraudster doesn't demand compliance from the victim, but draws him into co-constructing the very evidence that will then compel him to become complicit in the acts required to defraud him.

The following extract is where the fraudster manoeuvres the victim into the final stage—into a position where he will engage in the actions that will lead to him unknowingly enabling the fraudster to have illicit remote access to his computer. The so-prefacing at the start of the following extract links the directive to the preceding information (extract 1d, line 201) as evidence for the next action required. The use of 'now' (line 210) highlights the immediacy of the action needed, while 'just' (line 210) minimizes the implications of the action; compelling urgency from the victim while minimizing cause for alarm.

Extract 1e

210. F: So now just have a look on your keyboard sir,

.

214. F: On the very extreme left hand side can you see the three T and
215. control T?
216. V: Yeah

217. F: And next to control T now what button do you see?
218. V: Windows
219. F: Yes absolutely sir. So you need to hold that windows … key and the
220. letter R, R for Romeo together sir.
221. V: Yeah,
222. F: And what can you see on the screen …?
223. V: Ah it's come up with run
224. F: Ah yes. Can you see inside that box it's come up with a white … box
225. where you write something inside, sir?

The fraudster keeps the focus on what the victim can see, rather than what he wants the victim to do, a distortion which distracts from his issuing of commands and makes it appear as if the victim is in control. The fraudster also uses this as an implicit demonstration of expertize; displaying his knowledge of what the victim will see on his screen in detail (lines 214/15, 224) and through affirmations of what he would expect the victim to see at each stage 'yes absolutely' (line 219) and 'Ah yes' (line 224). The fraudster continues the call-and-response interaction seen in the previous extracts from this case, but the outcome has, unbeknownst to the victim, now become high-stakes. It is in this interaction he is directed to open up the 'run' command box—the channel through which the fraudster can gain remote access to the victim's computer. Following this extract, the fraudster dictates the individual letters for the victim to type into the command bar, therefore concealing the full name of the software that, when typed in and run, will give the fraudster remote access to the victim's computer.

Case 2

Case 2 is from a phone call from a fraudster posing as an agent from an insurance company, calling under the guise of informing customers of an opportunity to save money on their policy. After initially reaching the victim's wife, he is passed on to the intended target of the call. Extract 2a opens with the fraudster introducing himself, then outlining the reason for the call. Rooting the interaction in the present through the use of 'today' (line 10), and continuing with 'as you've got one year left with us' (lines 10, 11), the fraudster reveals the victim's status as the basis of the interaction. This has a four-fold impact; it highlights the immediacy of the situation and the uniqueness of the call to the recipient, reinforces the fraudster's legitimacy as a company professional (through demonstrating knowledge of details of the victim's contractual terms), and implicitly positions the victim as having 'earned' the call, rather than the fraudster seeking to be allowed to continue by the victim. This obscures the potential initial concerns of recipients of unexpected communications by deflecting the focus from the fraudster (Carter 2015); in this case, by redirecting the question of credibility from the fraudster and onto the victim.

Extract 2a

7. F: Hello, Mr Draper. It's Steve, calling from British Home Care. And it
8. was regarding your kitchen appliance breakdown cover.
9. V: Oh yes.
10. F: So the purpose of my call today is I wish to inform you that as you've
11. got one year left with us, we're going to be lowering the cost on your
12. agreement, so we're going to save you some money for the
13. remainder of the year.
14. V: Oh, thank you.
15. F: Right. Alright. I've got your address as number 2 Street name?

16. V: Correct.
17. F: [postcode]?
18. V: Yes.

Similar to extract 1a, the follow-up detail that builds on this opening introductory statement sets out the fraudster's intentions and the victim's position relative to this, with 'so' (line 11) situating this talk as the next in a series of turns, linked by a continuing narrative (Johnson 2002). The fraudster uses the floor to produce statements of intent and responsibility: 'I wish', 'you've got' and 'we're going to' (lines 11–14). He demonstrates knowledge of the customer's contract in accounting for the call ('you've got one year left with us', lines 11–12), which, together with the formality of the talk ('inform you', line 11), and the formulaic nature of the opening, establishes the legitimacy of the caller as a representative of the organization.

The premise of the call, in offering a reduction in bills, is a benefit as observed in frauds and described as the 'good Samaritan' approach by Kikerpill and Siibak (2021), the unexpected nature of which is reflected in the victim's 'oh' (line 14). Similar to extract 1b, the reduction in costs isn't framed as an offer presented to the recipient to accept or reject, but as an inevitability ('we're *going to* be', line 12). The victim is implicitly compelled to remain in the interaction with the fraudster in order to benefit, with the use of 'today' (line 11) suggestive that this opportunity is limited to that day (and therefore that call), which skews effective decision making (Busemeyer and Townsend 1993). Without an alternate source of advice or assistance outside the immediacy of this call, the victim is driven into acting to secure this readily-available opportunity for help offered by the service provider (whose job it is to locate and resolve these very issues). Restricting the options available to the victim serves to narrow their attention and focus, and compromizes their ability to engage in rational decision-making (MacFarlane et al. 2020).

The fraudster then, on line 15, moves the talk from providing information to requesting information; this potentially alarming move mitigated through it being a contextually-relevant request (although this isn't explicitly topicalized by the fraudster), and also by this being framed as a request to confirm information known by the caller, rather than a request for the recipient to provide *new* information. Subsequent to this, the fraudster escalates the request-confirm framework by asking the victim to describe the appliances in his house, an act that involves him physically navigating the building.

The fraudster's 'I've been able to' (line 61) refers to this 'work' he has just performed to secure a discount for the victim. This is linked to his previous interaction with the victim through the use of 'so', suggesting the caller's efforts to reduce the price relied on the customer's co-operation in providing details of the items in his home. Interestingly, the caller's effort to reduce the cost appears at odds with the seemingly straightforward, guaranteed reduction mentioned at the outset ('we're going to be lowering the cost' line 11).

Extract 2b

61. F: … So, I've been able to reduce the price down to £120. For the year.
62. V: Right.
63. F: Okay? For your appliances, covered until July 2020.
64. V: Thank you.
65. F: Your policy will end. Just to make you aware, your policy will
66. stay the same, which includes unlimited cover. No extra to pay on
67. repairs or parts. And if an engineer can't repair your appliance, we'll
68. offer you a cash settlement or replacement free of cost. Okay?

69. V: Thank you.
70. F: Okay. So, all that's left is for me to review the payment. So I'll
71. need you quickly to confirm your three-digit number on your card.

Lines 65-68 show the fraudster going through standard terms, genre-mapping (Carter 2015) legitimate requirements of organizations when invoking a change in contract. 'Okay' (line 70) orients the listener to the overall structure of the talk, specifically signalling a new element of a continuing narrative (Rendle-Short 1999). Together with 'so', the fraudster's turn links the reduction in cost and the next stage in the process ('for me to review the payment', line 70) in order for that reduction to happen. It is in this way that the fraudster pre-accounts for his request for sensitive data (the victim's bank card CVC code) that will enable and directly lead to the theft of his money, as an ordinary and required next step. The use of 'quickly' (line 71) although topicalizing urgency, serves to minimize the seriousness of the fraudster's request, reframing it as something that can be performed almost out-of-hand, rather than something that requires thought. This is a distraction from the reality which is the fraudster is requesting card details that will enable him to defraud the victim. It also minimizes the importance of this step in completing the fraud. The significance of the request in terms of it requiring the victim to expose themselves to harm is minimized by the fraudster explicitly referring to this request as a 'review' and a procedural 'need', (line 71), and by presenting it as information the victim must 'confirm' (line 71) which is already known; implying there is no risk of exposure in terms of providing information, a request that has been normalized by prior, benign requests to confirm details (line 15, 17, extract 2a).

Case 3

In the first extract, the fraudster poses as a member of a bank's security department, calling the customer as they have identified suspicious account activities, and now need to complete some steps with the customer to ensure their account is secure. Similar to extracts 1a and 2a, the fraudster introduces himself and the company, and the reason for the call. He then goes into further detail about the call, using 'so' (line 9) as a narrative continuer which links his prior statement of credibility and the statement of risk to the victim and implicit talk of future risks. Following his introductions, the fraudster opens the conversation by providing reassurances to the victim, framing the as-yet unidentified issue (referred to ominously as 'some activities' on line 9 and again on line 10) as already made safe, and the reason for the call to make sure the victim *remains* safe and 'completely protected' (line 17). The significance of this is the threat therefore remains possible as the victim is yet to receive the 'latest technology security' (line 17), and the fraudster is using the threat of a potential (repeat) future attack to compel the victim to remain on the phone to do so. Agreeing to perform a distinctly risky action (providing bank card details) is presented as an inevitability, rather than an option ('we will be verifying all your details', line 16), and a requirement in order to keep the victim safe.

Extract 3a

1. V: Hello?
2. F: Hello. Am I talking to Mr Williams?
3. V: Er, yes.
4. F: A very good day, sir. And how are you doing today?
5. V: I'm fine, thank you.
6. F: That sounds good. Well, I'm sure, this is Harry Adams calling you from

7. Nationwide Building Society security's department.
8. V: Oh yes?
9. F: Alright. So, sir, we have noticed some activities, and as you know that
10. you are absolutely secured now, before there was some activities
11. happen, but now you are absolutely secure. Now, we are giving-we
12. have given you this call because we have updated the securities and
13. the protection for you against international scammers and hackers,
14. okay?
15. V: Thank you.
16. F: We will be verifying all your details in order to update you with the
17. latest technology security, so you are completely protected.
18. V: Thank you.

The 'as you know' (line 9) is reminiscent of the 'must have noticed' (extract 1d, line 187) in its overt assumptive claim to the victim's knowledge. Information presented as expected to be known is difficult to challenge. It is also used in a similar way to extracts 1a and 2a, where the call is predicated on the fraudster's knowledge of the victim's status. Similar to extract 2a, the non-problematized compliance is gained from the victim through the lens of confirmation; the caller has the details, and the victim is to 'verify' (line 16) they are correct, in a type of reciprocal demand whereby the caller requires the recipient to provide the details so that they can equip the recipient with the protections of the 'the latest technology security' (lines 16–17) they need to keep safe.

In extract 3b, the request then takes the form of confirming details already known to the fraudster, rather than a request for new information. This reduces the perception of risk and, additionally, supports the credibility of the fraudster's cover story as he demonstrates knowledge of the victim's card details and address, which genre-maps what would be expected knowledge from a genuine communication from a bank's security department.

Extract 3b

22. F: Okay. That's your address, [says address]?
23. V: Yes
24. F: [says postcode]. And I have your card number starting with [says four
25. numbers]
26. V: That's correct, yes.
27. F: And I have your card number. Your Visa Mastercard? [says card
28. number]. And I have your Flexi-card [says card number]
29. F: Okay. No problem.
30. F: Yeah, okay. Alright. So, you have the card with you now?
31. V: Yes.
32. F: Perfect. Just confirm the long 16-digit number, should number starting
33. with [4 digits]. [Pause] Oh which card you handy with, sir? The one
34. which is starting with [same 4 digits]? Or [different 4 digits]? Which one
35. you handy with?

The fraudster's informal 'which one you handy with' (lines 34/35) belies the high stakes nature of what the victim is being asked to do and creates the illusion of control; it is the victim's decision which bank card to use. However, this decision-making is restricted in terms of choosing a card, rather than whether or not to provide sensitive information.

DISCUSSION

In each case considered here, the fraudster first establishes initial compliance from the victim (extracts 1a, 2a, 3a), then works to ensure continued compliance (extracts 1b, 1c, 1d) and to move into more risky territory without causing concern (extracts 1e, 2b, 3b). Fraudsters compel action from the victim by demonstrating their expertize, from which the victim will benefit financially (case 2) or in terms of security (case 1 and 3). The specialized knowledge claimed by the fraudster means the victim is relieved of the responsibility of assessing the utility of the tasks they are being asked to perform. Limiting decision-making is central to compliance because obedience is closely linked to an individuals' (in)ability to exercise initiative (Cohen 2001). Explicit and implicit claims to knowledge can be used as a tool powerful enough to compel a suspect to respond to police questioning against their best interests (Carter 2013), and the present research shows that in fraudulent interactions they are also performed in explicit (extracts 1c, 1d, 2a, 3b) and implicit (extracts 1b, 1c, 1d, 1e) forms which are used to compel the recipient to comply with requests that will allow their exploitation. In the opening extracts of each of the cases, the fraudster demonstrates their 'credibility' through identifying themselves as a legitimate representative of an organization, and providing explicit justifications for the contact (1a, 2a, 3a). As the interaction develops, fraudsters demonstrate knowledge of the victim's address and postcode, under the guise of confirming these are the correct details (extracts 2a, 2b, 3a, 3b) using requests to 'confirm' details as a way to request information without causing alarm. Reverse, assumptive claims to knowledge (extracts 1d, 3a) are also used to compel agreement from the victim or risk losing face. This framework of request-comply then normalizes later requests for information that expose the victim to risk of financial exploitation. The fraudster also obscures the reality of choice available to the victim and their agency in relation to this by presenting otherwise concerning requests (such as requests for bank card details or to navigate their computer) as unproblematic and already agreed. In extracts 1b and 2a, the victim's decision-making is misdirected; disguised as a choice in relation to details of the agreed action, rather than agreeing whether to perform the action in the first place.

By framing their actions as acting out the requirements of the (fictional) role they hold in the organization they purport to represent (extracts 1a, 1c, 1d, 3a), the fraudster recasts demands as conduits rather than sources of the directive, in a type of 'othering' that is particularly effective in reducing alarm in scam communications (Carter 2015). The contact from the fraudster is not posed as an offer but as a requirement or formality, making it difficult to challenge (Carter 2015). The interactional and social difficulty in rejecting the fraudster's contact is compounded through the 'good Samaritan' (Kickerpill and Siback 2021a) nature of the offer (security and protection from threat (case 1, case 3), or a discount on an agreed and contracted service (case 2). The 'shock and awe' (Kickerpill and Siback 2021a) of stating that scammers have already infiltrated their lives (case 1), and the implicit suggestion that an offer is time limited (case 2) also contribute to the compulsion to comply, through invoking the 'hot state' of panic and fear, which compels quick decision making and actions. A sense of urgency prevents individuals from cognitive processing that can lead to discrepancies in the interaction to be overlooked, or if identified, not followed-up (Wang et al. 2012), 'increase errors in decision making and [lead to an] increased likelihood of poor decision making' (Wang et al. 2012: 348). However, direct demands for urgency could alert the recipient to the fraudulent nature of the interaction. The analyses reveal the fraudster creates a sense of urgency but avoids doing so explicitly by using the present tense to root the issue in that moment and highlight it as a current concern (extracts 1b 2a, extract 1b) and frame it as a situation requiring immediate action (extract 1c). Direct references to speed are present, however these are counter-intuitively used to minimize the gravity of the action being performed, as something to get done without much thought ('quickly',

extract 2b), or a direct reference to waiting for the victim, but in the wider context of this not being a concern (extract 1b).

In all three cases, the fraudster inverts the burden of legitimacy away from themselves and onto the victim, by topicalizing the victim's eligibility for the call, of victim as having 'earned' or 'qualified' for the contact from the fraudster (extracts 1a, 2a, 3a), disrupting the question of credibility from the fraudster and on to the victim. In extract 1a, the victim qualifies as a receiver of the information and help due to his legitimacy as a genuine user of the software, whereas in extract 2a the victim's legitimacy is due to his status as a customer contracted to the company. In extract 3a, the victim 'qualifies' for additional security because their account has been subject to ominous 'activities'. This reinforces the credibility of the fraudster (as an assessor of eligibility) and draws the victim away from early concerns about caller legitimacy, and towards the exclusivity of the call and seizing its benefits. These range from protecting the computer (extract 1), receiving a discount on contracted services (extract 2) protecting a bank account (extract 3).

Direct threats can motivate the receiver into action (Williams and Polage 2018), however in fraudulent communications, using overt threat or making unsubstantiated claims to authority risks driving the victim to question the authenticity of the communication and expose it as a fraud (Kikerpill and Siibak 2021). The fraudster mitigates this risk by issuing threats within the framework of indirect talk about harm (it has been visited on others in the same geographical area as the victim, lines 11–12, extract 1a) and direct threats couched in vague ominous references ('some activities', line 9, extract 3a). This, and the overarching narrative of threat as a type of othering, is important in their mitigation. Othering is also present in the framing of threats as situations the fraudster can remedy; used in extract 1d to mitigate the prior overt, immediately present direct threat to the victim's online safety (extract 1c). Threat and authority can therefore be leveraged successfully to compel compliance from victims, with concerns anticipated and mitigated through direct and indirect claims to authority such as acting on behalf of a company, displaying knowledge of the victim's details or situation, and offering to provide expertize that they need to rely on in order to ensure their safety from cyber-attack (case 1 and 3), or provide financial relief (case 2). By situating the interaction within a wider frame of helping the victim (by identifying a danger, cases 1 and 3; or an opportunity for savings, case 2), the fraudster can harness the concept of reciprocity and its associated sense of trust and obligation (Carter 2015) to take compliance beyond the benign and to the point of harm. The faux-collaborative nature of the interaction disguises its one-sided nature in terms of power and the fraudster's demands. This is performed through co-opting the victim into the joint 'discovery' of evidence for further action (case 1), making the victim's co-operation with the fraudster's requests match the fraudster's efforts to achieve them a discount (extract 2b), and in both fraudster and victim working together to match the details held by both parties in order to achieve a joint goal (extracts 2a, 3b).

So-prefacing (present in all extracts) and minimizers such as 'just' (extracts 1a, 1b, 1d, 1e, 2b, 3b), also enable fraudsters to frame their requests as a normal, non-threatening part of a wider, legitimate requirement. Within this framework, the victim is drawn into navigating their computer (case 1), and their home (to take an inventory of their insurable goods, case 2; and to physically locate their bank card, case 3). It is here where the fraudster normalizes physical compliance, while implicitly indicating that he is not in control and is reliant on the victim's knowledge to assist them; creating the illusion that it is the victim that is in control of their information and of the environment, and minimizing cause for concern. This positive framing is present through each interaction; the victim is in control and discovers the issue, and the fraudster as the facilitator, who only seeks confirmation. This is seen in the fraudster minimizing their requests (extract 1b, 1e, 2a, 2b, 3a 3c), and, where directives are given or requests made, these are justified explicitly (1b, 1d, 3a) or implicitly (1c, 2b, 3b).

CONCLUSION

This research has examined the ways in which fraudsters create a social and interactional reality where victims feel reassured of the legitimacy of the communication and compelled to comply with acts that ultimately culminate in their own exploitation. With an assumption of truth as the default (Levine 2019), if a communication is frictionless in terms of not causing the victim concern, or if potential concerns are addressed (Carter 2015), then personally and financially damaging compliance can be successfully compelled from victims.

Fraudsters use social and interactional expectations to manoeuvre individuals into compliance without causing alarm, through manipulating power relations and harnessing interaction, social compliance and normative perceptions of roles to 'genre map' (Carter 2015) legitimate credible communications. Further, in a type of acculturation (Stubbins Bates 2014), fraudsters exploit social and interactional expectations to displace victims into a false reality through which they are then defrauded. Fraudsters also build a victim's commitment to the interaction where they become drawn into being part of the fact finding with the fraudster, with actions and decisions appearing co-constructed by the fraudster and the victim. This ostensibly joint enterprise validates the legitimacy of both context and content due to the victim being integral to the interaction's success. Knowledge of legitimate contexts and their associated social and interactional expectations are used by fraudsters as the very tool through which victims are compelled to act against their best interests.

Compliance, once established, is used to normalize further, now risky requests reminiscent of 'escalation commitment' (Dorison et al. 2022) which is the compulsion to match the efforts of the other party. When understood as a type of grooming that has similarities to domestic violence and abuse and coercive control (Carter 2021), it becomes incongruous to responsibilize the victim to protect themselves from manipulation and exploitation, and frame victimhood as a failure of self-protection. Particularly when we consider that victims of this crime report suffering multiple long-term psychological impacts including PTSD (Whitty and Buchanan 2016), and victims who describe the manipulation as so intrusive and psychologically harmful as to be akin to rape (Deem 2000; Whitty and Buchanan 2016). Public facing guidance often describes becoming a victim of fraud as something that individuals have 'fallen for', and associated narratives that responsibilize individuals to protect themselves from crime are useful where self-protection is clear, accessible and achievable (locking your car, not leaving valuables on view to prevent opportunistic vehicle theft or theft from your vehicle). The inadequacy of narratives of responsibilization in relation to the lived reality of victimhood (Carter 2021) and misrepresenting the ease with which one can protect oneself from fraud contributes to negative and shaming victim-blaming discourses surrounding victims of this crime (Cross 2015). This in turn negatively impacts victims' fraud-reporting (Button et al. 2013). The lack of any consistent fraud victim aftercare pathway, or agreement that there should be one, also belies the reality of fraud victimization as a pervasive crime that is psychologically as well as financially damaging. The potentially injurious nature of these crime prevention strategies and lack of aftercare following reporting is particularly pertinent when we consider that fraud is a crime where victim participation is needed for the fraudster to gain access to and extort an individual's money or data, and by this standard, any victim of fraud therefore will be deemed to have failed to perform the requisite standard of self-protection required to avoid victimhood.

Drawing on interactional frameworks to understand the manipulation from a social level, this research represents the beginning of important work towards more sustainable understandings of fraud victimization that move away from discrete situations of vulnerability to societally-wide susceptibilities, consistent provision of aftercare for victims, and more accurate and effective protection and prevention work that is driven by accurate narratives of fraud victimhood. By revealing the wider frameworks through which compliance is sought,

achieved and maintained, this research takes a step away from traditional perceptions of victims as different, vulnerable individuals. It moves towards a new understanding that frauds are not necessarily irregularities or deviations from 'normal' interactions that can be identified for their oddity and stopped. This exposes the responsibility-driven narratives of fraud protection literature as not only misplaced but also inadvertent drivers for negative narratives around self-protection and blame; damaging discourses repeated and replicated in popular public narratives that rationalize criminality as a consequence of a victim's lack of cognitive capacity or the flagrant, greedy or foolish making of bad decisions (Cross 2015). This research starts to progress academic and practitioner discourse beyond individualized definitions of vulnerability that can inadvertently deny legitimacy of victims that do not fit the expected or 'ideal victim' of this crime (Christie 1986) in terms of age, agency in the crime and whether or not the victim exhibited a reasonable level of self-protection (Cross 2015). It has potential wider, societal impacts as it strikes at the heart of the underlying negative narratives around victimhood and blame of the victim, signifying a move towards dispelling the shame felt by victims (Button et al. 2013), which would reduce a significant barrier to reporting. This work has also shown that social, ethical and interactional norms and expectations are harnessed and exploited by fraudsters; redefining understandings of victims' compliance and laying bare the principles through which the very narratives around fraud victimhood and the efficacy of fraud protection strategies must be reconsidered.

REFERENCES

Association of Chief Trading Standards Officers (ACTSO). (2014), *Summary of Doorstep Crime Report to National Tasking Group*. London: ACTSO.

Bidgoli, M. and Grossklags, J. (2017), *'Hello. This is the IRS Calling.': A Case Study on Scams, Extortion, Impersonation, and Phone Spoofing*. 2017 APWG Symposium on Electronic Crime Research (eCrime), 57–69.

Burchel, G. (1996), 'Liberal Government and Techniques of the Self', in A. Barry, T. Osborne and N. Rose, eds, *Foucault and Political Reason: Liberalism, Neo-Liberalism and Rationalities of Government*, 19–36. London: UCL Press.

Buil-Gil, D. and Zeng, Y. (2021), 'Meeting You Was a Fake: Investigating the Increase in Romance Fraud during COVID-19', *Journal of Financial Crime*, 29: 460–75.

Busemeyer, J. R. and Townsend, J. T. (1993), 'Decision Field Theory: A Dynamic-Cognitive Approach to Decision Making in an Uncertain Environment', *Psychological Review*, 100: 432–59. doi: 10.1037/0033-295x.100.3.432

Button, M., Lewis, C., and Tapley, J. (2009), *Fraud Typologies and Victims of Fraud. National Fraud Authority*; available online athttps://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdf

Button, M., Nicholls, C. M., Kerr, J. and Owen, R. (2014), 'Online Frauds: Learning from Victims Why They Fall for These Scams', *Australian & New Zealand Journal of Criminology*, 47: 391 –408.

Button, M., Tapley, J., and Lewis C. (2013), 'The "fraud justice network" and The Infra-Structure of Support for Individual Fraud Victims in England and Wales', *Criminology & Criminal Justice*, 13: 37–61.

Carter, E. (2013), *Analysing Police Interviews: Laughter, Confessions and the Tape*. London: Continuum.

Carter, E. (2015), 'The Anatomy of Scam Communications: An Empirical Analysis', *Crime, Media, Culture*, 11: 89–103.

Carter, E. (2021), 'Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud', *British Journal of Criminology*, 61: 283–302.

Christie, N. (1986), 'The Ideal Victim', in E. A. Fattah, ed., *From Crime Policy to Victim Policy*, 17–30. London: Palgrave Macmillan.

Cialdini, R. B. (2007), *Influence: The Psychology of Persuasion*. New York: Collins.

CIFAS (2020), '*Romance Fraud: Fall for the Person not the Profile*'; available online at https://www.cifas.org.uk/insight/fraud-risk-focus-blog/romance-fraud-person-not-profile [Accessed 27 January 2022].

Cohen, S. (2001), *States of Denial: Knowing about Atrocities and Suffering*. Cambridge: Polity Press.

Crime Survey for England and Wales (2019), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019 Office for National Statistics [Accessed 12 July 2022].

Cross, C. (2015), 'No Laughing Matter: Blaming the Victim of Online Fraud', *International Review of Victimology*, 21: 187–204. doi: 10.1177/0269758015571471

Crown Prosecution Service (2022), https://www.cps.gov.uk/crime-info/fraud-and-economic-crime [Accessed 11 July 2022].
Deem, D. L. (2000), 'Notes From the Field: Observations in Working with the Forgotten Victims of Personal Financial Crimes', *Journal of Elder Abuse and Neglect*, 12: 33–48. doi: 10.1300/j084v12n02_05
Dorison, C. A., Umphres, C. K. and Lerner, J. S. (2022), 'Staying the Course: Decision Makers who Escalate Commitment are Trusted and Trustworthy', *Journal of Experimental Psychology General*, 151: 960–5. doi: 10.1037/xge0001101
Fox Tree, J. E. (2002), 'Interpreting Pauses and Ums at Turn Exchanges', *Discourse Processes*, 34: 37–55. doi: 10.1207/s15326950dp3401_2
Garland, D. (1996), 'The Rise of Risk', in R. V. Ericson and A. Doyle, eds., *Risk and Morality*, 48–86. Toronto: University of Toronto Press.
Heritage, J. and Sorjonen, M-L. (1994), 'Constituting and Maintaining Activities across Sequences: And-Prefacing as a Feature of Question Design', *Language in Society*, 23: 1–29.
Johnson, A. (2002), 'So…?: 'Pragmatic Implications of So-Prefaced Questions in Formal Police Interviews', in J. Cotterill, ed., *Language in the Legal Process*. London: Palgrave Macmillan.
Jones, H. S., Towse, J. N., Race, N. and Harrison, T. (2019), 'Email Fraud: The Search for Psychological Predictors of Susceptibility', *PLoS One*, 14: e0209684. doi: 10.1371/journal.pone.0209684
Kidwell, M. and González Martínez, E. (2010), '"Let me tell you about myself ": A Method for Suppressing Subject Talk in a "soft accusation" Interrogation', *Discourse Studies*, 12: 65–89. doi: 10.1177/1461445609346771
Kikerpill, K. (2021), 'The Individual's Role in Cybercrime Prevention: Internal Spheres of Protection and Our Ability to Safeguard Them', *Kybernetes*, 50: 1015–26.
Kikerpill, K. and A. Siibak (2021), 'Abusing the COVID-19 Pan(dem)ic: A Perfect Storm for Online scams', in J. C. Pollock and D. A. Vakoch, eds., *COVID-19 in International Media: Global Pandemic Perspectives*, 249–58. Oxon: Routledge.
Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D. Mottola, G., Carstensen, L. L., and Gotlib, I. H. (2018), 'Emotional Arousal may Increase Susceptibility to Fraud in Older and Younger Adults', *Psychology and Aging*, 33: 325–37.
Langenderfer, J. and Shimp, T. A. (2001), 'Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion', *Psychology & Marketing*, 18: 763–83.
Levine, T. R. (2019), *Duped: Truth-Default Theory and the Social Science of Lying and Deception*, University Alabama Press.
Maggi, F. (2010), 'Are the Con Artists Back? A Preliminary Analysis of Modern Phone Frauds', 10th IEEE International Conference on Computer and Information Technology, 824–31. doi: 10.1109/CIT.2010.156.
MacFarlane, D., Hurlstone, M. J. and Ecker, U. K. H. (2020), 'Protecting Consumers from Fraudulent Health Claims: A Taxonomy of Psychological Drivers, Interventions, Barriers, and Treatment', *Social Science & Medicine*, 259: 1–15.
Microsoft.com (2022), *Event Viewer-- What is Going on in Your Computer*; available online at https://answers.microsoft.com/en-us/windows/forum/all/event-viewer-what-is-going-on-in-your-computer/fdda2010-d4df-4fed-863b-89ce0142419d.
Naksawat, C., Akkakoson, S., and Loi, C. K. (2016), 'Persuasion Strategies: Use of Negative Forces in Scam e-mails', *Journal of Language Studies*, 16: 1–17.
Nguyen, C., Jensen, M. L., Durcikova, A., and Wright, R. T. (2021), 'A Comparison of Features in a Crowdsourced Phishing Warning System', *Information Systems Journal*, 31: 473–513.
Proofpoint (2019) *Human Factor Report 2019*. Proofpoint, Inc.
Rendle-Short, J. (1999), 'When "okay" is Okay in Computer Science Seminar Talk', *Australian Review of Applied Linguistics* (print edition), 22: 19–33.
Reyna, V. F. (2021), 'A Scientific Theory of Gist Communication and Misinformation Resistance, with Implications for Health, Education, and Policy', *Proceedings of the National Academy of Sciences*, 118: 15.
Roe, C. A. (1996), *Persuasion in the Context of a Psychic Reading. PhD Thesis*. Edinburgh: University of Edinburgh. https://era.ed.ac.uk/handle/1842/29972 [Accessed 23 June 2022].
Rowland, I. (2002), *The Full Facts Book of Cold Reading*, 3rd edn. London. England: Ian Rowland Limited.
Stubbins Bates, E. (2014), 'Sophisticated Constructivism in Human Rights Compliance Theory', *European Journal of International Law*, 25: 1169–82.
Teegavarapu, S., Summers, J. D., and Mocko, G. M. (2008), 'Case Study Method for Design Research: A Justification', *International Design Engineering Technical Conferences and Computers and Information in Engineering (IDETC-CIE)*, 47: 495–503.

Titus, R. M. (1999), 'The Victimology of Fraud', Paper Presented at the Restoration for Victims of Crime Conference Convened by the Australian Institute of Criminology in Conjunction With Victims Referral and Assistance Service and Held in Melbourne, September 1999. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.505.1706&rep=rep1&type=pdf [Accessed 20 June 2022].

Tzani-Pepelasi, C., Nilsson, M. G., Lester, D., Pylarinou, N. R., and Ioannou, M. (2020), 'Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics', *Journal of Forensic and Investigative Accounting*, 12: 163–78.

Wang, J. Herath, T. Chen, R., Vishwanath A., and Rao, H. R. (2012), 'Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email' *IEEE Transactions on Professional Communication*, 55: 345–62.

Whitty, M. T. and Buchanan, T. (2016), 'The Online Dating Romance Scam: The Psychological Impact on Victims—Both Financial and Non-Financial', *Criminology & Criminal Justice*, 16: 176–94.

Williams, E. J. and Polage, D. (2018), 'How Persuasive is Phishing Email? The Role of Authentic Design, Influence and Current Events in Email Judgements', *Behaviour and Information Technology*, 38: 184–97. doi: 10.1080/0144929x.2018.1519599