Journal of Forensic and Investigative Accounting
Volume 12: Issue 1, January–June 2020

Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics

Calli Tzani-Pepelasi
Mirjana Gavrilovic Nilsson
David Lester
Ntaniella Roumpini Pylarinou
*Maria Ioannou**

1. Introduction

For centuries fraudsters have been putting great thought into developing fraudulent systems, stories, and techniques to scam consumers and victimize individuals who fall into the scammer's traps (e.g., see the Spanish Prisoner) (Barnes, 2017; Croall, 2008; 2009; Mears, Reisig, Scaggs, and Holtfreter, 2016). Today's interconnected world and cheap methods of communication such as e-mail, telephone, and the Internet have become useful tools for offenders to execute various types of fraudulent activities such as scams. The OFT (2006) defines scams as a misleading or deceptive business practice, where individuals receive an unsolicited or uninvited contact (e.g., by e-mail, letter, phone, or advertisement) and false promises. Such practices allow scammers to swindle targeted individuals out of money or other valuable objects (p. 12).

1.1. Scam Types and Scammers' Motivation

There are many types of scams, and the *modus operandi* (MO) of offenders can vary significantly (Gordon and Buchanan, 2013). Action Fraud (2018), the UK's National Reporting Center for Fraud and Cybercrime, have an A-Z directory containing over 50 types of scams, which include identity theft, romance fraud, miracle cure and slimming cure scams, tax fraud, phishing, online scams (e.g., 419 scams), spam e-mails, and even fraud recovery fraud. Other common scams are sweepstakes and prize draws, doorstep crime and government agency scams, such as IRS/HMRC scams, on which this research focuses (Button, Lewis and Tapley, 2009; Lister and Wall, 2006).

Government agency scams involve fraudsters impersonating government officials and posting official-looking letters and e-mails, or making phone calls, during which they either ask for a payment of, for example, a fine, basing their demands on certain legislation, or ask for credit or debit card information for a tax refund (Action Fraud, 2018; "Bogus government agency scams", n.d.).

HMRC/IRS scams are based on a technique called phishing—sending e-mails or making phone calls that appear to be from reputable sources with the goal of gaining personal and financial information. This information is then stored in a database, which is used to scam individuals into paying large amounts of money (Banoff and Lipton, 2005; Hadnagy, Fincher, and Dreeke, 2015; Kaniuk, 2016). The fraudsters also may pressure individuals to wire money directly through companies such as Western Union and MoneyGram (Federal Trade Commission, 2014).

1.2. Financial Impact

The financial impact suffered by organisations or individuals as a result of scams can be severe. For example, UK Finance (2018) reported a £731.8 million loss in 2017 from unauthorised financial fraud across payment cards, remote banking and cheques, and a £236 million loss in authorised push payment (APP) scams. According to the Annual Fraud Indicator (AFI), frauds and scams cost the UK £190 billion annually (Muckett, 2017). In the U.S., the Consumer Sentinel Network, a unique investigative cyber tool, received 2.7 million reports of fraud including identity theft, imposter, and debt collection scams. This totalled $905 million of fraud losses with the most common type of reported fraud being debt collection; followed by identity theft and impostor scams (Federal Trade Commission, 2018).

Moreover, the Crime Survey for England and Wales (CSEW) estimated 3.2 million incidents of fraud in the year ending March 2018. The CSEW is thought to be the best measure of fraud offences directly experienced by individuals in England and Wales, as it measures a wide range of fraud offences including attempts and incidents not

*Authors 1, 3, and 4 are affiliated with the University of Huddersfield, U.K.; author 3 is at Stockton University; and author 2 is affiliated with the University of Manchester, U.K. We thank Dr Nataly Papadopoulou for offering her valuable insight in terms of how the law deals with HMRC/IRS frauds.

reported to the police. Furthermore, the CSEW incorporates fraud data collated by the National Fraud Intelligence Bureau (NFIB) from three reporting bodies: Action Fraud, Cifas, and UK Finance. However, these reporting bodies tend to only include reports on more serious cases, or cases which the victim deemed serious enough to report. Hence, fraud offences referred to the authorities make up only for a small proportion of the overall fraud offences (ONS, 2018).

1.3. Underlying Reasons for Victimization

Anyone can become a victim of a scam. However, scams tend to be customised to fit the profile of the individuals being targeted (OFT, 2006). This profile is one of the reasons that older people, for example, are exceptionally targeted. The assumptions that they are wealthier or that they may be socially isolated, cognitively impaired or bereaved make them easy targets for scammers (Age UK, 2015). Henderson, Sheppard, Lachs, Burnes, Zhao, and Pillemer (2017) found that elder financial fraud and scams is a common problem in the U.S., affecting approximately one out of every 18 cognitively intact, community-dwelling older adults each year. Consumer Sentinel Network annual report, on the other hand, found that younger people between the ages of 20 and 29 reported losing money to fraud more often than older people (FTC, 2018).

Victims of fraud may suffer financially, psychologically, and emotionally, with some individuals even attempting suicide due to embarrassment, shame, and anger (Age UK, 2015; Button, Nicholls, Kerr, and Owen, 2014). Embarrassment and shame also may explain the difficulty in assessing the prevalence rates of HMRC/IRS scams because individuals decide to conceal their victimization (Age UK, 2015; Thornton, Hatton, Ralph, and Owen 2005) or because they have not realized that they were scammed (Gorden and Buchanan, 2013).

1.4. HMRCIRS Scams

Recently, the Treasury Inspector General for Tax Administration (TIGTA) released a semi-annual report to Congress detailing that IRS impersonation scams continued to top the IRS's "Dirty Dozen" tax scams (see IRS, 2018). As of March 2018, 13,162 individuals had reported paying IRS impersonators a total of more than $65.6 million (TIGTA, 2018).

In the UK, government agency scams, and predominantly HMRC scams, made up a big portion of the £768 million of financial fraud in 2016 (Torney, 2017). Several news articles have reported on the staggering losses incurred by these scams, warning taxpayers to be vigilant about whom they receive phone calls or e-mails from (BBC News, 2017; Bromley, 2018; Mendoza, 2011; Pavia, 2016; Rosenberg, 2018). The IRS is attempting to warn taxpayers to be cautions of such scams, particularly before, during and soon after the tax-filing period. Other countries such as Canada and Australia have seen an increase in tax phone scams with scammers impersonating officials from the Canada Revenue Agency (CRA) and the Australian Taxation Office (ATO) indicating that tax scams may be growing into a global problem (Australian Taxation Office, 2019; Baugh, 2018).

1.5. Scammers' Characteristics and the Steps to a Successful Scam

All types of scams follow a well-delineated pattern with slight variations to achieve their goals (Langenderfer and Shimp, 2001). First, potential victims need to be identified. Potential victim lists are usually drawn from open source directories such as phone books, share registers of public companies, advertisements in personal columns, media articles about wealthy people, and by using a 'suckers' list which contains personal information of individuals who have previously been scammed (Button, Lewis, and Tapley, 2009; Levi, 2008). Personal and financial information also can be retrieved via phishing, phone calls, e-mail or websites that pose as legitimate sites (Kaniuk, 2016). The information is then stored in a database, or the "sucker's list", which is used to scam individuals repeatedly (Banoff and Lipton, 2005).

Scammers base their potential win not only on the abundance of the listed names in the "suckers' list", but they also are able to handle high emotional states and hide fear and stress, and they attain these by drawing on their personality resources and training or experience (e.g., persuasiveness and audacity, knowledge, tools, or 'crime facilitators'). Through deception and misinformation, scammers aim to turn a simple transaction into an overcomplicated situation to confuse individuals, making it harder for them to stay objective and recognise the scam (Button et al., 2009; Langenderfer and Shimp, 2001).

One of the reasons why individuals fall for scams is because of their legitimate appearance (Bidgoli and Grossklags, 2017; Button et al., 2009; Button, Nicholls, Kerr, and Owen, 2014; Employee Benefits, 2016). In the Olivier, Burls, Fenge, and Brown (2015) study on victims of mass marketing fraud, it was found that individuals initially become involved in scams because they seem to come from legitimate sources. Portraying a legitimate appearance and developing a trusting relationship with the victim is part of the scammer's toolkit. To appear legitimate scammers may modify the caller ID to mimic the number of a real company or organization, also known as caller ID spoofing (HMRC,

2019), and operate during tax-filing periods when individuals might believe that calls from tax organizations are more likely to occur (IRS, 2018).

Another reason why individuals fall for scams is because of pressure and coercion by scammers. Individuals are intimidated to go along with the scams by threatening, for example, arrest, imprisonment, license revocation, deportation and more (Button et al., 2014; IRS, 2018; Langenderfer and Shimp, 2001). In Button et al.'s (2014) study using focus groups, they found that "appeals to trust and authority" was one of the main reasons for why individuals fall for online frauds. This reason also is noted by research from the Office of Fair Trading (2006) and Whitty (2013). In HMRC/IRS scams, scammers frequently impersonate people or institutions of authority to make the scam appear legitimate and make the threats of intimidation more credible (Bidgoli and Grossklags, 2017).

Available research shows that scammers tend to have good sales skills and can persuade individuals that the phone calls are legitimate in order to get them to cooperate with their demands. Many scams take on the structure of legitimate call centres to operate as a 'boiler rooms' (Button et al., 2009). Scammers work as a team to make the scam successful (Phillips, 2016). The structure involves sales agents, closers, and re-loaders, just as in a legitimate telemarketing company, that use a scripted pitch to entice individuals into going along with their scam (Shover et al., 2003).

In many cases, scammers working as part of big, illegitimate, operation centres, do not have previous sales experience, having been recruited via attractive newspaper advertisements or through acquaintances with promises of high incomes and weekly incentives (Button et al., 2009). Many also join without knowing about the illegal activities they are aiding and only find out after joining For example, a former worker at a fake call centre that was shut down in Mumbai, India, told Reuters news agency that she took the job without knowing the centre's fraudulent activities, and she continued working there due to the high salary and weekly incentives given by operating managers (Jadhav, Rocha, and Bhatia, 2016).

In their 7th Annual Call Centre Fraud Report, Pindrop Labs (2017), a private company that helps call centres protect themselves against fraud, found that 64 percent of fraud calls originate outside the target countries. Moreover, in Bidgoli and Grossklags's (2017) IRS phone scam case study, they found that many callers often had a Middle Eastern or Indian-sounding accent and were mostly male. If a victim receives multiple phone scam calls, from individuals with a foreign accent, and a persistence in their attempt to have the victim pay "owed taxes", the victim can become cognisant of the scam, and thus the accent undermines the scammers legitimate appearance (Bidgoli and Grossklags, 2017; Button et al., 2009). Organizations also have highlighted this factor in their warnings and guides on how to recognise tax phone scams (Banoff and Lipton, 2008; Phillips Erb, 2014).

Although, many scams are a type of external fraud by organized and well-trained and prepared criminals, it is difficult to determine the extent of involvement of organised criminals because of their lucrative measures to avoid detection (Button et al., 2009). External fraud operations can consist of a single individual, two or three persons operating together, or a larger number of people working collectively in makeshift office facilities or call centres which mirror legitimate operations. These organized crime groups operate as a collective organization conducting 'boiler room' type operations where the group uses sale tactics, works together in a hub, such as a rented space with desks and telephones, and engages in fraudulent activities and scams on an industrial scale (Button et al., 2009; Henderson, 2003; Levi, 2008). These types of operations, especially larger telemarketing fraud setups, have similar characteristics to legitimate operations with hierarchies, division of labour and wages (Levi, 2014).

As mentioned above, many scammers are based overseas, which makes it more difficult for authorities to locate the fraudsters (private investigators are sometimes used to locate fraudsters), obtain extradition (see the UK's government extradition: processes and review guidance in 2013), mount a prosecution, or recover any compensation (Grabosky and Smith, 1996). Certainly, there are exceptions, and there are several cases of successful prosecutions and extradition of individual fraudsters. Some recent examples include: Olanrewaju Bolaji Otukoya in 2018, Vijay Mallya in 2018, and Daniel O'Connell in 2019. Some governments also are unlikely to cooperate across borders unless the scamming operations are large in scale (Baugh, 2018; "Scammed by a foreigner, what are my legal options?", 2018), such as the operation closed down in India in 2016 (see Jadhav et al., 2016). Attempts, however, are made for cross-border investigations and combating corporate crime and fraud (for instance, see New Corporate Crime, Fraud, and Investigations multi-jurisdictional guide, 2012).

In countries where there is limited police interest for scams, limited investigating resources and weak sentencing, scammers flourish with more opportunities to commit fraud and conceal their activities (Albrecht, Albrecht, Albrecht and Zimbelman, 2011). An example is Spain, where police interest in scams and organised fraud has been low in recent years (Button et al., 2009; Levi, 2014). There is evidence that many IRS/HMRC scams may take place overseas

as well. Just this year, 21 people were sentenced in a multimillion-dollar call centre scam based in India that ran between 2012 and 2016, targeting thousands of U.S. victims by impersonating officials from the IRS (Department of Justice, 2018). Scammers also may move locations regularly to avoid detection. This tactic is often called 'rip and tear' where scammers use multiple locations that function as mobile offices, from which they conduct their activities. Disposable mobile devices and prepaid calling cards tend also to be used. Many boiler room operations function this way (Button et al., 2009; Levi, 2014; National White-Collar Crime Centre, 2008). Seeking small sums of money at a time is another tactic, which makes reporting the event to the police unlikely (Button et al., 2009; Langenderfer and Shimp, 2001).

Fraud has not been a priority for law enforcement (Levi, 2008; Cross and Blackshaw, 2014). Victims often avoid reporting frauds and scams because of ignorance, embarrassment, or self-blaming (Bidgoli and Grossklags, 2017; Button et al., 2009) and, consequently, IRS/HMRC scams are significantly under-reported. Since many of the fraudulent units are not based in Western countries, locating, arresting, and collecting information about these scammers becomes extremely difficult. This explains the limited empirical research on the offender profile and characteristics of HMRC/IRS scammers. The need for understanding the behaviour, motivation, and tactics of these criminals, necessitates further research. The present study utilises unconventional means to collect data on these scams in order to raise awareness and protect the public from further victimisation.

1.6. The Present Study—Aim

It is evident from the literature review that there has been an increase in researching HMRC/IRS phone scams in the past few years (e.g., Bidgoli and Grossklags, 2017). However, to our knowledge, there has not been a study on the offender profile of HMRC/IRS scammers. Because of this research gap, the present descriptive/qualitative exploratory study is the first step to introduce offender profiling into the field of tax phone fraud. The research aim of this article is to build an offender profile and identify the characteristics of HMRC/IRS scammers.

Motivated by the severe financial consequences as well as the emotional consequences for victims from scamming of both individuals and organizations, the lack of data and available research, the repetition of victimisation and limited awareness, this project explores the various ways, in which IRS/HMRC scammers commit these crimes in order to shed light on the offenders' characteristics.

2. Method

2.1. Data

The detection-avoidance strategies mentioned earlier are the main reasons that law enforcement cannot detect and/or locate these scammers, thereby posing a difficulty for detailed research. However, even if they were to be located, they would most likely be unwilling to reveal their scamming techniques. Based on the latter consideration, for this project the research team used a rather unconventional method to study the IRS/HMRC scams and access data. The researchers used 30 YouTube videos. YouTube videos have been used for empirical studies in the past (e.g., Adami, 2009). In these videos, trolls engaged in discussions with the HMRC/IRS scammers. Trolls have not been extensively studied and their role is still to be defined (De Seta, 2013; Phillips, 2013). However, in Internet slang, a troll is a person who sows discord by starting arguments, upsetting people or posting inflammatory, extraneous or off-topic messages in an online community (such as a newsgroup, forum, chat room, or blog), with the intent to provoke other users into an emotional response for the amusement of the troll. In this study, some of these trolls are legitimate taxpayers who were contacted by scammers to victimize them. The trolls took the matter personally, located the fraudulent HMRC/IRS numbers that scammers used and called the fraudulent numbers to troll them and waste their time. Other trolls realized that they were being scammed but chose to play along and waste the scammer's time. These individuals believe that, the longer they keep the scammer on the line, the less likely another innocent taxpayer is victimized. Trolls are referred in this study as victims although their victimization was not successful, while their persona also aligns with Internet vigilantism.

2.2. Video selection

To retrieve YouTube videos containing trolls engaging with HMRC/IRS scammers from YouTube, a search was performed using the following key words: 'IRS tax scamming', 'HMRC tax scamming', 'trolling tax scammers', 'tax scamming', 'phone tax scamming'. The search resulted in several videos, which contained trolls engaging in a phone conversation with HMRC/IRS scammers who believed that the trolls were genuine targets. The dates of the videos that were selected ranged from 2016 up to December 2018. After a thorough examination of the videos resulting from the search, only 30 videos were selected with the following criteria:

1. Videos were longer than three minutes
2. The troll engaged into a discussion with the scammer and the scamming technique was revealed

3. The trolls were mature and serious individuals and did not contact the scammer just to insult them
4. The videos were in English
5. The content of the videos was solely related to the IRS/HMRC scams

The researchers limited the inclusion of some of the other videos mainly because the videos needed to have enough communication time for the scammers to reveal some of the characteristics prior to realizing that he/she was being trolled. For consistency, the researchers had to maintain the strict selection criteria.

2.3. Speaker Profiling

Speaker profiling is used as a forensic investigative tool when there is an unknown offender, and investigators need to narrow down the suspect pool by identifying linguistic features and speech patterns that can be linked with geographical areas, social groups or pathologies, for example, smoker's voice (Schilling and Marsters, 2015; Watt, 2010). Experts or 'speech analysts' use a variety of methods, such as aural-perceptual, acoustic phonetic or automated analysis to carefully examine voice quality, rhythm and speech patterns using quantitative, objective and replicable methods which are often more accepted by courts as valid expertise (Watt, 2010). However, speaker profiling also is performed by non-experts or "naïve" listeners who use simple auditory analysis, that is, listening, to build a profile, and so must rely on previous experience of voice and language variety (Watt, 2010).

In this research, speaker profiling was used by listening to ascertain a scammer's characteristics such as gender, accent and language use, including sentence structure and verb tense, to gain some insight into the individuals who might be committing the IRS/HMRS scam calls. Other characteristics identified were related to the techniques used to persuade potential victims that the call is legitimate and thus comply with monetary demands.

3. Results—IRS/HMRC Scam Characteristics

From the 30 YouTube analysed videos, 26 IRS/HMRC offender characteristics were identified and are explained below in detail.

3.1.1. Gender. For the 30 cases, 27 (90%) scammers were male and three (10%) female. Gender was identified by listening to the voice of the scammer and the name provided.

3.1.2. Accent. For the 30 cases, 19 (63.3%) included scammers who did not have a clear or native British-English or American-English accent, 11 (36.7%) had a type of English accent that could perhaps persuade non-native English speaking victims that the scammer is calling from the IRS or HMRC, 25 (83.3%) had an Asian-type of English accent, four (13.3%) had a clear English accent, but without clarity of the accent being American or British, and one (3.3%) had a Jamaican-English accent.

3.1.3. Language syntax and grammar. The sentence structure was examined, particularly whether the English language was spoken correctly (e.g., verb tense, correct articles chosen, etc.). Fourteen (46.7%) of the scammers made grammatical mistakes constantly during the entire troll-scammer conversation, and 16 (53.3%) made some grammatical mistakes (e.g., "as I say to you before, your case and papers will be inside the courthouse, your papers were laying down in the post office").

3.1.4. Threats/intimidation. The threats that the scammers used were as follows: two used no threats, two used personal threats (e.g., "your kids will be taken away from you"), 26 (80%) used threats such as imprisonment, arrest, social media exposure, freezing of assets and bank accounts, passport and driving license revocations, house seizure and property possession.

3.1.5. Surrounding Environment/Background. In 27 (90%) of the calls the background included noise that resembled a call centre. However, it cannot be confirmed if these were other scammers online with potential victims, or fake background noise purposely recorded to persuade victims that the call is indeed coming from a government agency. Only 3 (10%) calls did not include such background noise and were relatively quiet.

3.1.6. Senior manager. In nine (30%) cases, the availability of a senior officer, supervisor or manager was not mentioned or asked for during the conversation, in two (6.7%) cases there was no senior officer, supervisor or manager available, and in 19 (63.3%) cases a senior officer, supervisor or manager was available and became involved.

3.1.7. Anger management. In 19 (63.3%) cases the scammer did not exhibit anger when provoked, confronted or exposed by the troll, in six (20%) cases they exhibited anger when provoked, confronted or exposed by the troll which led to insults and vulgar language, and in two (6.7%) cases the scammer ended the call when provoked, confronted or exposed by the troll.

3.1.8. Remorse. In 22 (73.3%) cases the scammer did not show any remorse for the fraudulent activity, six

(20%) showed remorse, and two (6.7%) ended the call before exposure and confrontation by the troll could take place. Remorse was measured by observing whether the scammer was remorseful and regretted their actions when exposed by the troll and whether he/she had any intention to discontinue their criminal lifestyle.

3.1.9. Payment method. In 16 (53.3%) cases the scammer asked the victim to buy an iTunes card to pay for the amount supposedly owed (this was solely in IRS scams), three (10%) asked for a bank transfer (HMRC scams), five (16.7%) did not reach the point during the call where they would actually provide details regarding the payment method, one (3.3%) asked for MoneyGram payment, two (6.7%) asked for cash withdrawal but did not reach the point in the conversation where they would instruct the victim what to do with the cash to complete the payment, two (6.7%) asked for debit card details to complete the payment (HMRC), and one (3.3%) asked for a stream card type of payment.

3.1.10. Contact. In 11 (36.7%) cases the scammer left a voice mail to the victim with a number to call back, four (13.3%) called the victim's mobile phone, one (3.3%) called the victim's landline, and in 14 (46.6%) cases calls were made by the trolls themselves and the numbers were then reported in YouTube or other online platforms as fraudulent numbers. It must be clarified that in 16 cases the victims were legitimate regardless of their choice to later engage in this trolling behaviour, while in 14 cases the trolls chose to impersonate a victim in order to engage with the scammers. Nevertheless, for consistency, legitimate victims and trolls are referred as victims throughout this article.

3.1.11. Call behaviour. In 28 cases (93.3%) the scammer put the victims on hold, pretending that he/she was checking the victim's criminal record or tax files, or asked for the victim to stay on the line whilst driving to the store to buy the iTunes cards or withdraw cash. Only two of the scammers did not wait on the line for any of the above reasons.

3.1.12. Communication persistence. Twelve (40%) scammers would not allow for a call-back or would call back themselves if the call was interrupted, 11 (36.7%) would allow a call-back or would call the victim back themselves, and only one did not mention anything about this option.

3.1.13. Victims' private information. Four (13.3%) scammers did not seem to have an address for the victim, four (13.3%) had the real address of the victim, 11 (36.7%) did not mention anything about an address, and 11 (36.7%) gave an actual address, but it was not the victim's.

3.1.14. Phishing. In 27 (90%) cases the scammers asked for personal information, including address, profession, personal savings, while only three (10%) did not do this.

3.1.15. Secrecy. In 10 (33.3%) cases the scammer asked the victim to keep the matter and the payment transaction confidential, 10 (33.3%) referred to confidentiality of the call but did not ask the victim to keep it a secret, and 10 (33.3%) did not mention secrecy at all.

3.1.16. Exhibiting fear. When exposed 21 (70%) did not show any kind of fear of being caught, six (20%) showed some kind of concern when exposed and confronted, two (6.7%) ended the call without any indication, while in one case the call was interrupted before the scammer could be confronted. An example of fear or concern from their discussion included, "If I lose this job, I will not be able to feed my family." An example of no fear or concern is, "Call whoever you want; you can't get to me."

3.1.17. Call excuse. In 27 (90%) of the cases the scammers told the victims that they owed money to the HMRC/IRS because of tax filling errors or miscalculations in previous reports, one (3.3%) did not give a clear reason, and two (6.7%) did not reach that point in the conversation to give a reason for the call.

3.1.18. Case reference number and a badge number. In six (20%) of the cases the scammer would not give a case reference number, in 15 (50%) of the cases, they provided a case reference number along with a badge number, and in nine (30%) of the cases, no reference number was mentioned.

3.1.19. Requested amount. In seven cases (23.3%) the conversation between the scammer and the victim did not reach the step where the scammer asks for the payment and informs the victim of the allegedly owed amount. The remaining 23 (26.7%) cases included the following amounts: $500, $800, £1500, $1626, $1800, $1900, $2400, £3994, $4000, $4649, $4981, $4986.73, $5200, $5562, $6435, $6850, $9600.78, $11070, $18251, $5453.40, $5982.32.

3.1.20. File. In 24 (80%) of the cases the scammer pretended to put the victim on hold for a few seconds in order to pull the relevant file from their database, while only six (20%) did not mention a taxpayer's file.

3.1.21. Identity. The scammers adopted personas and had given their characters the following names: Blake O'Connor, Derek Johnson, Erik Wilson, James Anderson, Jenifer, John Cooper, John Green, Jordan Smith, Larry Holmes, Mark Terens, Michael, Michael Lynn, officer Johnson, Officer Kevin Matgamont, Officer Christianson, Paul

Davis, Paul Smith, Richard Butler, Robert Peel, Norman, Sharkai Glowscow, and Sierra Courtney. In seven cases, the scammers did not give a name and refer to themselves as an IRS or HMRC officer.

3.1.22. Location. When confronted, some of the scammers revealed the location of this fraudulent operation. Two (6.7%) scammers revealed their location as Pakistan, two (6.7%) as India, 22 (73.3%) did not give their location, one (3.3%) insisted that he was calling from Washington, and one (3.3%) from England.

3.1.23. Vulgar and insulting language. In 17 (65.7%) of the cases the scammer did not use insulting language when confronted or exposed, in 12 (40%) of the cases they used insults and vulgar language, and one (3.3%) scammer did not react either way when confronted.

3.1.24. Patience. In 27 (90%) cases the scammer showed patience and listened to all sorts of stories that victims used in order to delay the scammer. One (3.3%) scammer became irritated from the beginning as well as during the confrontation, and two (6.7%) did not reach the point in the conversation that would require patience with the victim. An example of being patient was when the troll would repeat the same question multiple times without the scammer getting irritated.

3.1.25. Inducing fear and intimidation. In 27 (90%) cases the scammer tried to induce fear in the victim, either by repeating the consequences of not complying with their demands or by adding new threats and, at times, even personalising them (e.g., after the troll pretended to be a single dad with two young girls, the scammer threatened that the police would take his kids away if he did not pay the allegedly owed amount). Only one (3.3%) scammer did not try to scare the victim further, and two did not have the chance to induce any fear as a result of the call ending.

3.1.26. Verbal aggression. In eight (26.7%) of the cases the scammer did not become verbally aggressive if irritated, while in 20 cases (66.7%) the scammer became verbally aggressive when irritated, delayed, confused, confronted or exposed. In two (6.7%) cases the scammer did not have the chance to react because the call ended. Verbal aggression was measured by the amount of vulgar and insulting language expressed by the scammers.

Figure 1 shows the overall scammer profile, and Table 1 summarizes the characteristics.

Figure 1. Summary of Scammers' Characteristics.

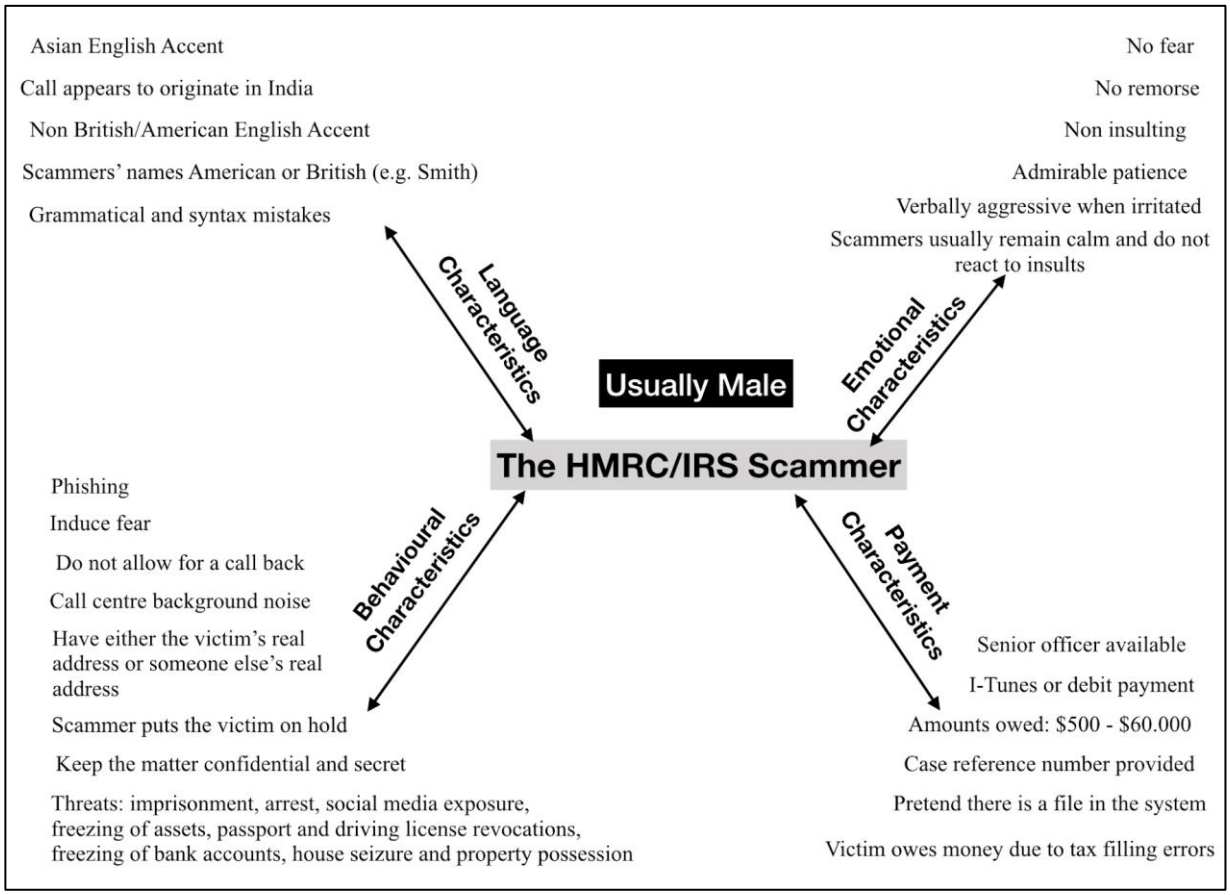

Table 1. Summary of Scammer Characteristics.

Variables	n	%
Gender of scammers		
Male	27	90.0
Female	3	10.0
Accent of scammers		
No clear/native British/American English	19	63.3
Convincing to non-native English speakers	11	36.7
Asian-type English	25	83.3
Clear English (no clarity on British or American)	4	13.3
Jamaican-English	1	3.3
Language syntax and grammar		
Grammatical mistakes	14	46.7
Some grammatical mistakes	16	53.3
Threats/Intimidation		
No threats	2	10.0
Personal threats	2	10.0
Other threats	26	80.0
Surrounding Environment/Background		
Background noise resembling a call centre	27	90.0
No background noise	3	10.0
Senior officer/supervisor/ manager		
Not mentioned	9	30.0
Mentioned but not available	2	6.7
Available and involved	19	63.3
Anger management when provoked/confronted/exposed		
No anger	19	63.3
Anger	6	20.0
Ended call when confronted by troll	2	6.7
Remorse for fraudulent activity		
No remorse	22	73.3
Some remorse	6	20.0
Ended call before exposure by troll	2	6.7
Payment method		
iTunes card (IRS scam)	16	53.3
Bank transfer (HMRC scam)	3	10.0
No payment method detailed	5	16.7
MoneyGram	1	3.3
Cash withdrawal	2	6.7
Debit card details asked for	2	6.7
Stream card	1	3.3
Scammer contact with victims		
Voice mail left for call back	11	36.7
Called mobile phones	4	13.3
Called landline	1	3.3
Trolls called scammers	14	46.6
Call behaviour		
Victims put on hold/Scammers wait online for payment	28	93.3
Did not put on hold/wait online for payment	2	6.7

Communication persistence		
Would not allow call-back/Would call back themselves if call interrupted	12	40.0
Would allow call-back/called back themselves	11	36.7
Option not mentioned	1	3.3
Victims' private information		
Did not have victim's address	4	13.3
Had victim's real address	4	13.3
Gave an address that was not from victim	11	36.7
Did not mention address	11	36.7
Phishing		
Asked for personal information	27	90.0
Did not ask for personal information	3	10.0
Secrecy		
Asked to keep matter and payment method secret	10	33.3
Only referred to confidentiality of call	10	33.3
Did not mention secrecy/confidentiality	10	33.3
Exhibiting fear when exposed		
No fear	21	70.0
Some concern	6	20.0
Ended call with no sign of fear	2	6.7
Call interrupted before exposure	1	3.3
Call excuse		
Victims' owed money	27	90.0
No clear reason	1	3.3
Did not reach that point in call	2	6.7
Case reference/badge number		
Case reference but no badge number provided	6	20.0
Both provided	15	50.0
None mentioned	9	30.0
Requested amount		
Did not reach point in call to request amount	7	23.3
From $500 to 5982.32	23	26.7
File		
Pretended to pull out relevant file	24	80.0
Did not mention any file	6	20.0
Identity		
Likely fake name provided	23	76.7
No name provided	7	23.3
Scammer location		
Pakistan	2	6.7
India	2	6.7
Washington DC	1	3.3
England	1	3.3
No location mentioned	22	73.3

Use of vulgar and insulting language by scammer when confronted/exposed		
None	17	65.7
Used	12	40.0
No reaction	1	3.3
Patience by scammer		
Was patient	27	90.0
Became irritated	1	3.3
Call ended before situation requiring patience	2	6.7
Inducing fear and intimidation		
By repeating consequences of not complying/Adding new threats	27	90.0
No intimidation	1	3.3
Call ended before any intimidation	2	6.7
Verbal aggression when irritated (by troll)		
None	8	26.7
Present	20	66.7
Call ended before reaction	2	6.7

Discussion

Taking into consideration the variety of scamming techniques that exist, the rapid development of new scams in line with technological advances, and the severity of financial losses and psychological consequences for victims, this study found value in identifying the characteristics of IRS and HMRC scammers and their scamming techniques.

As previously stated, after a thorough examination of the literature on scams and scamming techniques, it was revealed that there is a clear research gap in terms of profiling HMRC/IRS scammers. As no other study has been identified that investigates the profile of HMRC/IRS scammers, this study attempted to use the limited literature on the subject as a steppingstone for further research on HMRC/IRS scams. This study has managed to provide a general profile of the characteristics of the scammers and tax scam calls, many of which correspond with the characteristics identified in Bidgoli and Grossklags's (2017) IRS phone scams case study. It should be mentioned that this study differs from the above-mentioned project as the latter provided a general profile of the scammers by interviewing victims, while the present study studied the victim-scammer interaction.

In terms of the characteristics, the first observation was that most scammers were male and did not have a British/English or American/English accent, which may indicate that the scammer did not reside in the same country as the victim. This might be a reason why these trolls quickly realized that the call was a scam. Bidgoli and Grossklags (2017) noted that foreign accents are traits that victims can become cognizant of if they have received multiple phone scams. This fact is something that organizations highlight in their warnings and guidance on how to recognise tax phone scams (Phillips, 2014). Even though they had non-English accents, they would still use typical English names such as John Smith or Robert Peel.

Foreign accents also may support the notion that many scams originate overseas (Department of Justice, 2018; Banoff and Lipton, 2008). In this study, some scammers revealed their location as being Pakistan or India. When scams originate overseas, it becomes difficult for authorities to locate the scammers, because governments are not likely to cooperate across borders unless scamming operations are large in scale, or because there is limited police interest (Albrecht et al., 2011; "Scammed by a foreigner, what are my legal options?", 2018).

The scammer identified many potential victims/trolls by leaving a voice mail warning the victim that the IRS/HMRC is about to take legal action against them. A call back from the victims is perceived as a potential win. The scammer then provided a case reference and badge number in half of the cases. The scammers also try to persuade their victim that they are legitimate representatives of the IRS/HMRC organizations. Authority and legitimacy have frequently been found to be a key trigger for scam victimisation (Bidgoli and Grossklags, 2017; Button et al., 2009; Button et al., 2014). The attempt by scammers to seem legitimate was evident in this study as well. In half of the cases,

a case reference and badge number were provided, in 90% of the cases the background resembled a call centre, and in 63% of the cases a senior officer, supervisor or manager was available and became involved.

Threats have constantly been found as a key feature of tax phone scams to pressure victims into paying the requested amount (Bidgoli and Grossklags, 2017; IRS, 2018). Threats featured heavily in these cases as well. Most troll/victims were threatened with imprisonment, arrest, and social media exposure, freezing of assets, passport and driving license revocations, freezing of bank accounts, house seizure, and property confiscation.

The scammers appeared to be experts at hiding their fear and stress (even when confronted) and exhibited patience during the call with the aim of gathering more information about the victim, which they can later use to intimidate or persuade victims into paying. They used wording that may sound official and, at times, confused the victim and overcomplicated a situation, thus making it harder to recognise that they are scammers (see Langenderfer and Shimp, 2001). The scammers kept up their professional, calm demeanour even when the trolls confronted them. However, many started using vulgar and insulting language, audibly annoyed with the troll for wasting their time.

Lastly, these scammers seem to be aware of the illegality of their actions, but some of them appear conflicted. In some cases, the scammer admitted that scamming is wrong but, in others, exhibited pride for their success and their fraudulent and persuasive skills. In the cases where scammers appear conflicted, they blamed their financial state and lack of other options for legitimate work and tried to persuade the victim that scamming was their only option for survival. In one case, however, the scammer reported that he had not initially been aware of the fraudulent nature of his work and intended to leave once he received his payment. This example supports the notion that large organized crime operations may hire individuals responding to attractive job ads promising payments but having no idea of the deceitful nature of the job (Button et al., 2009). From the scammers who willingly revealed information about the nature of this scamming technique, apparently, these scamming organizations have their bases away from city centres and areas where transportation is available. They also implied that the employees are living within the operations facilities and do not visit their homes frequently. Therefore, it appears that these organizations are carefully established with a possible hierarchy in place and funding available to organize and sustain the scam and to train, feed and pay these employees (see Button et al., 2009; Levi, 2008).

Limitations and Further Research

The exploratory nature of this study presents a limitation in terms of reliability and validity. However, as previously explained, there has not been previous empirical research that attempts to profile HMRC/IRS scammers. Despite this limitation, this study can function as a steppingstone for future research and further development of this field. Because the study focuses on HMRC/IRS scams, it cannot be generalised to other countries apart from the US and the UK. Perhaps future research could attempt to profile scammers that operate against other Western countries such as Australia and Canada.

Using only 30 YouTube videos for the descriptive analysis presents a further limitation in terms of the strengths of the inferences being made as well as the generalizability of the results. However, many of the YouTube videos obtained from the search were inadequate for research purposes, as the troll betrayed his deceitful nature of the call to the scammer from the start. Therefore, many of the videos that were identified but not included in this study could not assist in identifying the scammer's characteristics. Future research could conduct a more thorough examination of a wider variety of trolling videos in order to identify a larger sample that could assist in strengthening the inferences made.

Moreover, at times the troll would reveal him/herself before the scammer had a chance to conclude the scam. Therefore, important information might have been missed regarding the *modus operandi* of the scammers. Nonetheless, trolls had uploaded the videos that were selected for this study, with millions of YouTube channel subscribers. Many of the subscribers commented on the videos, revealing their own scam experiences similar to the ones taking place in the videos, and others commented that these videos had made them aware of these scams and the techniques and so were able to protect themselves when faced with similar phone calls.

Implications

The results of this study can be used to enhance public awareness of tax phone scams. The findings provide valuable insights into recognising tax scams and particularly for prevention of further victimisation. The study also alerts the public to the risk of scams and alerts taxpayers that they should not instantly believe the word of unsolicited calls and rush into detrimental decisions. In addition, it provides better information about the modus operandi used to exploit innocent taxpayers, including offender characteristics, which can aid authorities in investigatory matters. Organizations, such as the IRS the HMRC and tax related organisations from other countries, can use this study to inform their tax payers of the risks that may occur by responding to such calls without confirming the alleged

information with their lawyer or tax office prior to making any kind of payments. Finally, people are advised to be vigilant if they receive persistent calls from individuals who have foreign accents (see Banoff and Lipton, 2008) and poor English language skills, make non-realistic threats, use wrong wording and foul language, request immediate payment with iTunes cards and similar gift cards or other types of payments that are not HMRC/IRS designated, ask for irrelevant information, require or/and even demand secrecy over the transaction, make personal threats, and exhibit mockery, disrespect and verbal abuse.

Victims of fraud should seek psychological support from the support groups that are available, including Age UK or Victims Support UK. Furthermore, victims also could seek legal advice from lawyers, who sometimes offer legal advice on pro bono basis, from their local Citizens Advice Bureaus or Universities' Legal Advice Clinics. If the general public reports more fraud cases, then this brings necessary awareness to the issue, and the public also will be able to recognise the characteristics that the scammers use. This overall awareness helps authorities to reduce and combat fraudulent activity in the future, both offline and online. In conclusion, hopefully, this project will inspire other researchers to conduct similar projects that will increase public awareness for such scams and prevent further victimisation and financial loses.

Conclusion

For centuries fraudsters have been defrauding individuals and organizations out of money and property using various fraud techniques and scams. The HMRC/IRS scam is only one of many scams that have increased during the last decade. Since most of the organised crime groups that perpetrate these scams operate in non-Western countries, there has not been an easy way to collect data and discover more about how these scams function and the characteristics of the scammers themselves.

The aim of this exploratory study was to present an offender profile of the HMRC/IRS scammers by identifying their characteristics. This research used a recent form of data in the form of YouTube videos because there is no current way of approaching the scammers themselves to collect more valid data. Interviewing the victims could result in subjective inferences. The researchers, therefore, analysed 30 YouTube videos in which Internet trolls engaged with real HMRC/IRS scammers to learn more about their characteristics and techniques used during the scam.

The qualitative analysis of the troll-scammer interaction in the YouTube videos resulted in identifying 26 scammer characteristics which can function as the basis for the future development of this research field. Despite the limitations, the results may assist in increasing awareness of HMRC/IRS scams and provide organizations with a tool for identifying scammers in the hope of helping prevent increased HMRC/IRS scam victimisation of vulnerable individuals and organizations. In addition, the present project and its results expand on the information provided by Bidgoli and Grossklags (2017) and others (Banoff and Lipton, 2008; Button et al., 2009; 2014; Phillips, 2014). The present study differs from previous research as it focuses on profiling the scammers through the direct observation of their interaction with a victim (the troll).

References

Adami, E. (2009) 'We/YouTube': Exploring sign-making in video-interaction'. Visual Communication, 8 (4): 379–400.

Age UK. (2015). *Only the tip of the iceberg: Fraud against older people—Evidence review*. London. Retrieved from https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at- home/rb_april15_only_the_tip_of_the_iceberg.pdf

Albrecht, W., Albrecht, C., Albrecht, C., and Zimbelman, M. (2011). *Fraud examination* (4th ed.). Mason, OH: Cengage Learning.

A-Z fraud. (2018). Retrieved from https://www.actionfraud.police.uk/a-z-of-fraud-category/other

Australian Taxation Office. (2019). Scammers impersonate ATO phone numbers. Retrieved from https://www.ato.gov.au/Media-centre/Media-releases/Scammers-impersonate-ATO-phone-numbers/

Banoff, S. I., and Lipton, R. M. (2005). Dirty dozen, part iv: This year's scams IRS does not want taxpayers to fall for. *Journal of Taxation, 102(5)*, 319.

Baugh, C. (2018, September 21). Organized crime in Mumbai responsible for popular CRA phone scam. *iPhone In Canada*. Retrieved from https://www.iphoneincanada.ca/news/cra-phone-scam/

BBC News. (2017, January 19). Cybercrime and fraud scale revealed in annual figures. *BBC News*. Retrieved from https://www.bbc.co.uk/news/uk-38675683

Bidgoli, M., and Grossklags, J. (2017, April 25-27). "Hello. This is the IRS calling:" A case study on scams, extortion, impersonation, and phone spoofing. In *2017 APWG Symposium on Electronic Crime Research (eCrime)*. Scottsdale: IEEE. Retrieved from http://10.1109/ECRIME.2017.7945055

Bogus government agency scams. Retrieved from https://www.nibusinessinfo.co.uk/content/bogus-government-agency-scams

Britt, P. (2008). Tax time: Phishing scams and schemes. *Information Today, 25(4)*, 1.

Bromley, S. (2018, May 17). HMRC scam warning: the latest con and five others to avoid. *Simply Business*. Retrieved from https://www.simplybusiness.co.uk/knowledge/articles/2018/05/the-latest-HMRC-scam-voice-mail/

Button, M., Lewis, C. and Tapley, J. (2009). *Fraud typologies and victims of fraud*. National Fraud Authority. Retrieved from https://researchportal.port.ac.uk/portal/files/1926122/NFA_report3_16.12.09.pdf

Button, M., Nicholls, C., Kerr, J., and Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, *47*(3), 391–408. doi: 10.1177/0004865814521224.

CBS News. (2015, March 4). Dangerous "IRS" scam unfolding on your phone. *CBS News*. Retrieved from https://www.cbsnews.com/news/dangerous-irs-phone-scam-unfolding-on-your-phone/

Cifas. (2017). *Fraudscape 2017*. Cifas. Retrieved from https://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/External-Fraudscape%20report%202017.pdf

Cross, C., and Blackshaw, D. (2014). Improving the police response to online fraud. *Policing*, *9*(2), 119–128. doi: 10.1093/police/pau044.

Crowe. (2018). *Crowe's latest global fraud research shows an epidemic costing the UK £110 billion–£3.2 trillion globally*. Retrieved from https://www.crowe.com/uk/croweuk/insights/financial-cost-of-fraud-2018

Cumbria Constabulary. (2016). Police warn of HMRC money scam. Retrieved from https://www.cumbria.police.uk/News/News-Articles/2016/May/Police-warn-of-HMRC-money-scam.aspx

Cumbria Constabulary. (2016). Police warn of HMRC money scam. Retrieved from https://www.cumbria.police.uk/News/News-Articles/2016/May/Police-warn-of-HMRC-money-scam.aspx

Department of Justice. (2018). 24 defendants sentenced in multimillion-dollar India-based call center scam targeting U.S. victims. Retrieved from https://www.justice.gov/opa/pr/24-defendants-sentenced-multimillion-dollar-india-based-call-center-scam-targeting-us-victims

Employee Benefits. (2016). *How employees could avoid losing their pension to scams and fraudsters*. London: Employee Benefits. Retrieved from https://search-proquest-com.manchester.idm.oclc.org/docview/1765447151?accountid=12253andrfr_id=Info%3Axri%2Fsid%3Aprimo

Federal Trade Commission. (2014). Government Imposter Scams. Retrieved from https://www.consumer.ftc.gov/articles/0048-government-imposter-scams

Federal Trade Commission. (2018). *Consumer Sentinel Network Databook 2017*. Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf

Federal Trade Commission. Consumer Sentinel Network. Retrieved from https://www.ftc.gov/enforcement/consumer-sentinel-network

Financial Fraud Action UK. (2018). *Cheque fraudsters involved in £1.8M scam jailed after being extradited to UK.* Retrieved from https://www.financialfraudaction.org.uk/news/2018/10/16/cheque-fraudsters-involved-in-1-8m-scam-jailed-after-being-extradited-to-uk/

Gorden, C., and Buchanan, J. (2013). A systematic literature review of doorstep crime: Are the Crime-Prevention strategies more harmful than the crime? *The Howard Journal of Criminal Justice, 52(5),* 498–515. doi:10.1111/hojo.12036.

Grabosky, P., and Smith, R. (1996). Fraud: An overview of current and emerging risks. In Australian Institute of Criminology, *Trends and issues in crime and criminal justice*. Canberra: Australian Institute of Criminology. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.569.9836andrep=rep1andtype=pdf

Hadnagy, C., Fincher, M., and Dreeke, R. (2015). *Phishing dark waters: the offensive and defensive sides of malicious e-mails*. Wiley.

Henderson, L. (2003). *Crimes of persuasion*. Azilda, ON: Coyote Ridge Pub. HMRC phone scam warning. (2016, July 20). [Blog]. Retrieved from https://www.cumbria.police.uk/News/News-Articles/2016/July/HMRC-phone-scam-warning.aspx

Holden, M. (2018, December 10). UK court orders Indian tycoon Mallya to be extradited on fraud charges. *Reuters UK*. Retrieved from https://uk.reuters.com/article/uk-india-mallya-britain/uk-court-orders-indian-tycoon-mallya-to-be-extradited-on-fraud-charges-idUKKBN1O91DQ

Home Office (2016). *'Extradition: processes and review' guidance by the UK Home Office.* Retrieved from https://www.gov.uk/guidance/extradition-processes-and-review

Internal Revenue Service. (2018). IRS wraps up 'Dirty Dozen' list of tax scams for 2018; Encourages taxpayers to remain vigilant. Internal Revenue Service. Retrieved from https://www.irs.gov/newsroom/irs-wraps-up-dirty-dozen-list-of-tax-scams-for-2018-encourages-taxpayers-to-remain-vigilant

Jadhav, R., Rocha, E., and Bhatia, R. (2016, November 29). Callers for dollars: Inside India's scam call centers. *Reuters*. Retrieved from https://www.reuters.com/article/us-india-fraud-usa/callers-for-dollars-inside-indias-scam-call-centers-idUSKBN13O2XZ

Kaniuk, R. S. (2016). Lawyer and IRS phishing e-mails become today's Nigerian e-mail scams. Experience: *The Magazine of the Senior Lawyers Division, American Bar Association, 26(3),* 10.

Langenderfer, J., and Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing, 18(7),* 763–783. doi:10.1002/mar.1029.

Levi, M. (2008). Organized fraud and organizing fraud: Unpacking research on networks and organization. *Criminology and Criminal Justice, 8*(4), 389–419. doi: 10.1177/1748895808096470.

Levi, M. (2014). Organized fraud. In P. Letizia, *The Oxford Handbook of Organized Crime*. Oxford: Oxford University Press.

Lister, S. and Wall, D. (2006) Deconstructing distraction burglary: an ageist offence.

Mendoza, M. (2011). Colorado Springs residents should beware of phony IRS e-mails, it is a scam. *The Colorado Springs Business Journal*.

Muckett, J. (2017, November 13). UK loses £190bn due to fraud. *Economia*. Retrieved from https://economia.icaew.com/news/november-2017/uk-loses-190bn-due-to-fraud

National White-Collar Crime Center. (2008). *Telemarketing fraud (October 2009)*. National White-Collar Crime Center. Retrieved from http://www.nw3c.org/docs/research/telemarketing-fraud.pdf?sfvrsn=6

Office of Fair Trading (2006). Research on Impact of Mass Marketed Scams: A Summary of Research into the Impact of Scams on UK Consumers (No. OFT883). Office of Fair Trading: London.

Office for National Statistics. (2018). *Crime in England and Wales: year ending March 2018*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018#overview-of-crime

Office for National Statistics. (2018). *Overview of fraud and computer misuse statistics for England and Wales*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25#how-are-fraud-and-computer-misuse-defined-and-measured

O'Riordan, A. (2019, January 15). Extradition of a Cork man in multimillion-euro fraud case 'is of very significant public interest'. *Irish Examiner*. Retrieved from https://www.irishexaminer.com/breakingnews/ireland/extradition-of-a-cork-man-in-multimillion-euro-fraud-case-is-of-very-significant-public-interest-897793.html

Pavia, J. (2016, October 18). Sadly, IRS phone scams are very successful 'businesses'. *CNBC*. Retrieved from https://www.cnbc.com/2016/10/18/sadly-irs-phone-scams-are-very-successful-businesses.html

Phillips, C. (2016). From 'rogue traders' to organized crime groups: Doorstep fraud of older adults. *The British Journal of Criminology, 57(3),* 608–626. doi: 10.1093/bjc/azw011.

Phillips Erb, K. (2014, March 21). IRS, TIGTA continue to warn taxpayers of 'Largest scam of its kind'. *Forbes*. Retrieved from https://www.forbes.com/sites/kellyphillipserb/2014/03/21/irs-tigta-continue-to-warn-taxpayers-of-largest-scam-of-its-kind/#235024b43b8d

Pindrop Labs. (2017). The geography of phone fraud: Where do phone scams come from? [Blog]. Retrieved from https://www.pindrop.com/blog/the-geography-of-phone-fraud-where-do-phone-scams-come-from/

PLC Cross-border (2012). *New Corporate Crime, Fraud, and Investigations multi-jurisdictional guide*. Retrieved from https://uk.practicallaw.thomsonreuters.com/3-5213194?transitionType=DefaultandcontextData=(sc.Default)andfirstPage=trueandcomp=plukandbhcp=1

Rosenberg, J. (2018, July 12). Is it the IRS, or a scam? Government issues taxpayer fraud warnings. *USA Today*. Retrieved from https://eu.usatoday.com/story/money/usaandmain/2018/07/12/irs-scam-government-fraud-warning-taxpayer/770198002/

Scammed by a foreigner, what are my legal options? (2018). Retrieved from https://www.hg.org/legal-articles/scammed-by-a-foreigner-what-are-my-legal-options-34916

Schilling, N., and Marsters, A. (2015). Unmasking identity: Speaker profiling for forensic linguistic purposes. *Annual Review of Applied Linguistics*, *35*, 195–214. doi: 10.1017/s0267190514000282

Shover, N., Coffey, G., and Hobbs, D. (2003). Crime on the Line. Telemarketing and the Changing Nature of Professional Crime. *British Journal of Criminology*, *43*(3), 489–505. doi: 10.1093/bjc/azg489

Thorne, B., and Stryker, J. (2015). *The "Dirty Dozen" tax scams plus 1*. Deland, FL: Stetson University. Retrieved from https://www.ship.edu/contentassets/569211b0c6f243808c3c64f54e816cd2/v7n1thornep1-p22.pdf

Torney, C. (2017, December 27). New phone scams and how to avoid them. Retrieved from https://www.saga.co.uk/magazine/money/spending/consumer-rights/scams/how-avoid-phone-scams

Treasury Inspector General for Tax Administration. (2018). *TIGTA Semiannual Report to Congress: October 1, 2017 – March 31, 2018*. Washington: Department of the Treasury. Retrieved from https://www.treasury.gov/tigta/semiannual/semiannual_mar2018.pdf

UK Finance. (2018). *Fraud the facts 2018: The definitive overview of payment industry fraud*. London. Retrieved from https://www.ukfinance.org.uk/wp-content/uploads/2018/07/Fraud-the-facts-Digital-version-August-2018.pdf

Wagner, N. (2007). Identity fraud profiles: Victims and offenders. *Eighth World Congress on The Management of Ebusiness*. doi: 10.1109/WCMEB.2007.50.

Watt, D. (2010). The identification of the individual through speech. In C. Llamas and D. Watt, *Language and identities* (1st ed., pp. 76–85). Edinburgh, Scotland: Edinburgh University Press. Retrieved from http://www-users.york.ac.uk/~dw539/watt2009.pdf

Wood, S., Liu, P., Hanoch, Y., Xi, P., and Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied*, *24*(2), 196–206. doi: 10.1037/xap0000167.