Accounting Forum xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Accounting Forum

journal homepage: www.elsevier.com/locate/accfor

Detecting advance fee fraud emails using self-referential pronouns: A preliminary analysis

Rofiat Alli, Rebecca Nicolaides, Russell Craig*

Portsmouth Business School, University of Portsmouth, Portsmouth, UK

ARTICLE INFO

Keywords:
Deception
Email
Fraud
Language
Nigerian

ABSTRACT

We promote awareness of the features of emails that propose advanced fee fraud schemes. These are commonly known as 419 emails (after Section 419 of the Nigerian Penal Code). We outline the structural features of 419 emails and conduct a preliminary study of their distinctive linguistic features, using word frequency counts and DICTION text analysis software. We find that the incidence of first person singular pronouns is seven times greater in 419 emails than non-419 emails. We suggest elements of a future research agenda that can build on our preliminary results to help reduce advanced fee fraud.

1. Introduction

Fraud is a misstatement or false representation that is intended to deceive for personal (usually financial) advantage (Action Fraud, 2010). Advance Fee Fraud (AFF) is the most frequently encountered and successful type of fraud in history (Ofulue, 2010; Garrett, 2014). AFF involves a request for advance fees or upfront payments by a dishonest person from a victim, for resources, goods or services that never materialise (Action Fraud, 2010; FBI, 2010; Ultrascan AGI, 2014a, 2014b). AFF schemes commonly employ two or more other kinds of fraud (such as impersonation fraud, identity theft, and/or phishing) (Edelson, 2003).

In this research note, we focus on a specific kind of AFF, known widely as *419 fraud.* This type of fraud is claimed to be "one of the longest running, most successful, omnipresent [and] transnational [frauds]… in history" (Ultrascan AGI, 2014b; p. 16). *419 fraud* involves:

> …scheme(s) designed by fraudsters purporting to have lucrative but bogus business, humanitarian or philanthropic related deals where the victim is promised large sums of money for no initial investment.… [and]… is persuaded to advance some cash to the scammer for a variety of purposes such as the payment of unanticipated taxes, duty fees and outright bribery. The victim will later discover that there is no fortune to be retrieved or business to profit from, as the scammer disappears with the advance fee he or she had collected (Onyebadi & Park, 2012; p. 182)

Attempts to perpetrate this particular type of fraud are regularly experienced by many members of society, including accountants and their clients. Indeed, typically, government regulatory agencies throughout the world advise persons who are suspicious of any email from a stranger seeking upfront payment of funds to seek advice from "an accountant or financial planner if in doubt" (Australian Competition and Consumer Commission, *Scamwatch* website, https://www.scamwatch.gov.au/types-of-scams/unexpected-money/inheritance-scams).

The research note that follows should be particularly beneficial in raising the consciousness and understanding of those with interests in forensic accounting, especially fraud detection. Our aim is to provide a portrait of *419 fraud* and to draw on that portrait

* Corresponding author at: Portsmouth Business School University of Portsmouth Richmond Building, Portland Street Portsmouth, PO1 3DE, UK.
E-mail addresses: Russell.Craig@port.ac.uk, Russell.Craig@vu.edu.au (R. Craig).

https://doi.org/10.1016/j.accfor.2018.01.003
Received 5 August 2017; Received in revised form 14 November 2017; Accepted 13 January 2018

to offer some preliminary insight to how *419 fraud* can be detected. We introduce the prospect that the computer aided text analysis software, *DICTION,* can assist in the detection of *419 fraud.* We do not canvass the theoretical underpinnings of fraud. For an understanding of this, see, for example, Choo and Tan (2007) and Schuchter and Levi (2015).

The term *419 fraud* originated in Nigeria and is derived from Section 419 of the Nigerian Penal Code that deals with false pretences (Nykodym & Taylor, 2004; Oriola, 2005; Salu, 2005). The term is used widely in international parlance to describe various fraudulent schemes perpetrated within or outside Nigeria (Adogame, 2009; Chawki, 2009). *419 fraud* has flourished for many decades and has defrauded thousands of "curious, naïve, and/or sympathetic" victims (individuals and companies) of cash and other assets — sometimes resulting in tragic mental health deterioration or even suicide (Glickman, 2005; p. 463). The extent of the monetary losses resulting from *419 fraud* has been estimated by Ultrascan AGI (Advanced Global Investigation). This is an international consulting firm comprising "51 partners managing 3,284 experts in 69 countries" which focuses on anti-money laundering and transnational organised crime (http://www.ultrascan-agi.com/public_html/html/about.html). According to Ultrascan AGI, by 2013, over $US 82 billion had been lost to *419* Advanced Fee Fraud, with $US 12.7 billion lost in 2013 ("419 Advance Fee Fraud Statistics 2013", http://www.ultrascan-agi.com/public_html/html/419_statistics.html). A recent case of AFF involved "a lonely [English] beancounter" who was jailed after "he fell for… a classic Nigerian email scam, and conned £150,000 out of a friend so he could bankroll his fake damsel in distress" (Martin, 2016).

Much legislation has been passed, especially in Nigeria, to curb *419 fraud*, but without success. Media education campaigns have encouraged the adoption of procedures (including recourse to the advice of accountants) to protect proprietary information and to lead to safer and more disciplined use of computers and the Internet. Several scam-baiting sites have also been developed, such as *419eater* (http://www.419eater.com/). Despite such efforts, there has been a strong increase in the perpetrators, victims, and losses from *419 fraud.* Nonetheless, the level of successful convictions of perpetrators has been low (Oriola, 2005). This is largely due to the difficulty in building a case against perpetrators because of technical aspects of the fraud (The Herald, 2017).

419 scammers (known as *419ers*) are adept at evading legal counter measures (Ultrascan AGI, 2014a, 2014b). Attempts to defeat them with traditional legal instruments have been inadequate due to the transnational nature of the fraud (Webster & Drew, 2017). The Internet has facilitated the activities of *419ers* because it offers a wider geographical coverage, access to a large number of potential victims at a low-cost and low-risk, new and readily available scamming opportunities, anonymity and concealment of identity through minimal physical contact (Blommaert & Omoniyi, 2006; Hutchings & Hayes, 2009; Ofulue, 2010; Webster & Drew, 2017). Dion (2010, p. 630) concluded that *419ers* regard the Internet as an "Eldorado" because of the "quasi absence of the rule of law." The failure of previous efforts to curb *419 fraud* prompted Holt and Graves (2007) and Herley (2012) to argue for the development of automated scam filter detection systems based on an understanding of how *419ers* think, and how their victims react.

In a forensic accounting context, the power of linguistic and psycholinguistic analysis techniques in understanding human behaviour reflected in fraud has been studied widely (see Nicolaides, Trafford, & Craig, 2018). Linguistic analysis techniques have been used to investigate behaviour associated with corporate fraud through study of CEO letters to shareholders, conference calls with financial analysts, and earnings press releases. These investigations have found some significant linguistic indicators of deception (Humphreys, Moffitt, Burns, Burgoon, & Felix, 2011; Craig, Mortensen, & Iyer, 2013; Purda & Skillicorn, 2015). Nonetheless, with respect to *419 fraud*, linguistic analysis is less developed, despite its strong potential for success (Ofulue, 2010; Carter, 2015). If *419 fraud* can be reduced considerably, it is claimed that this would help curtail undesirable associated activities such as money laundering, organised crime, corruption, and terrorism (Ultrascan AGI, 2014a, 2014b).

Here we conduct a preliminary exploration of how linguistic analysis techniques (including those involving the use of computer assisted text analysis) can be helpful in identifying a distinctive marker of *419 emails.* We are motivated by the promptings of Holt and Graves (2007), Herley (2012) and Lamberger, Dobovšek, & Slak (2013) to improve the rate of detection. In particular, we conduct a preliminary investigation of a sample of *419 emails* and *non-419 emails* using a linguistic cue that has been associated with deceptive conduct in written text: a high rate of use of first person singular pronouns. Thus, we address the following specific research question:

Is the incidence of first person singular pronouns substantially higher in 419 emails than in non-419 emails?

The central purpose is simply to draw attention to the importance of linguistic analysis techniques (particularly pronoun use) in helping to identify fraud. In doing so, we contribute to the accounting literature by introducing a wide variety of research on email fraud that has been published in other disciplines, such as in communications, social psychology, criminology, law and ethics. We propose some elements of a future research agenda.

Section 2 reviews literature on the nature of *419 emails*, how *419 fraud* is perpetrated, and outlines some studies of language use that have investigated whether pronouns are indicators of deception. Section 3 describes the research method. Section 4 presents results. Section 5 enters conclusions and offers suggestions for future research.

2. Literature review

2.1. The nature of 419 fraud

419ers use techniques that distort recipients' rational thought processes, and command a shift in behaviour by them (Freiermuth, 2011a, 2011b). These techniques are implicit in the structure and style of *419 emails*, where every word and sentence has a planned purpose (Ofulue, 2010; Freiermuth, 2011a, 2011b; Carter, 2015).

Scammers often obtain names and addresses of potential victims from trade journals, professional and commercial directories, lists in URLs and newspapers (Glickman, 2005). Some studies suggest that the preferred type of victim is an educated citizen (Lamberger et al., 2013; Ultrascan AGI, 2014a,b), whilst others contend that scammers prefer to target people who are elderly,