You Can Trust Me: An Exploratory Analysis of the Nigerian Email Scam

Timothy S. Rich
Assistant Professor
Political Science
Western Kentucky University
Timothy.rich@wku.edu

Working Paper
August 23, 2015

Abstract:

The advance fee fraud (AFF) scam (also known as the Nigerian or 419 email scam) has not only proliferated over time, but to the casual observer, there appears little meaningful variance in these scam appeals. This analysis challenges the conventional wisdom using a multi-method approach. Content analysis of over a half million scam emails reveals the rates of references to location, the monetary offers, and trust language employed. Experimental evidence suggests that trust rhetoric within scam letters has minimal influence on respondents' perceptions of the letter, but does affect recall. This analysis expands our understanding of the scam letter format and suggests means to further combat fraud.

Introduction

How should scholars analyze the advance fee fraud (AFF) scam? The AFF is known by many names, including the Nigerian or 419 email scam (in reference to Nigeria's penal code). While offers to share inheritances or release long dormant moneys in foreign banks are commonplace within the scam, the monetary offers vary considerably. The commonality among divergent narratives is the scammer's claim that various fees—described as taxes, bribes or other variations—are necessary before the larger sum can be released to the dupe. The scam ends when the dupe fails to continue paying such fees. Despite far-fetched premises not only have these scams proliferated, but to the casual observer, there appears little meaningful variance in these scam appeals. Even with greater spam detection programs, such emails remain commonplace.

Rather than treat the scam email as static, this analysis proposes a multi-method approach using a body of actual scam email letters and an experimental design based on similar letter templates.

While often mocked in popular culture, the AFF or Nigerian email scam not only funds criminal elements, potentially undermining the control of several states, but the association of the scam with Nigeria and Africa more broadly undermines efforts of international aid for the region. As such, a closer analysis of the mechanics of the fraud should provide several insights. The losses from these scams are non-negligible. Estimates since the 1990s range from $2 billion to nearly $10 billion a year (Legard 2002; Smith 2009; Cheng 2010; US Secret Service 2002). Over 55,400 individuals lodged complaints to the US Federal Trade Commission in 2005 alone regarding such scams (Bergiel et al. 2008), with a reported one in ten Americans losing money in such a scam in 2005 (Rosato 2006). Estimates of the average amount scammers fleece from victims varies widely from a few thousand to hundreds of thousands of dollars (e.g. Lazarus 2003; Schiesel 2004; Viosca et al. 2004; Longe et al. 2009). Prosecuting also remains difficult due to the lack of physical evidence, scammers who frequently changing email addresses (FraudAid ND),[1] and that the fraud often requires the victim to assist in activities of questionable legal status, potentially decreasing one's willingness to report later losses.

A sizable literature in business and computing deals with avoiding email scams (e.g. Barron 2006; Bergiel et al. 2008), but little social science research delves into the politics or the logic behind these scams. Social psychology research gives some insights into the actions of those scammed (Simon 1956; Tversky and Kahneman 1974; Kahneman and Tversky 1979; Kuhnen and Knutson 2005) and why once on the hook, victims often continue to give money. A parallel can be seen in Shefin and Statman (1985) in identifying the tendency of investors to "sell winners too early and ride losers too long" so as to resist acknowledging losses that reaffirm

errors in earlier decisions (also see Thaler 1980). Serial victimization is not uncommon, with those previously scammed often still caught off guard by later attempts. Furthermore, strong evidence reaffirms that individuals are far poorer at detecting deceit than they personally believe (Babad and Katz 1991).

Several important puzzles remain. Are there patterns within the texts of such scam emails and if so, what does this potentially tell us about both the scammers and the scammed? In particular, what is the role of trust appeals in the scam narrative? To tackle these questions, this paper analyzes over a half-million scam emails through automated content analysis, providing the largest quantitative study of the topic to date. Secondly, an experimental web survey provides individual level evidence regarding the perceptions of the AFF appeals, both in terms of the appeals to trust but also the amount offered. Ultimately, this article provides a multi-faceted analysis of the email scam phenomenon through methodological approaches increasingly common in social science yet unexplored on Nigeria scams.

This article will first briefly introduce the history and basic motivation within the Nigerian scam. Next is a discussion on how to analyze these scams in a more rigorous manner. Content analysis finds clear correlations in references to trust based on the claimed region of origin for the author and the monetary offer in the email. In contrast, an experimental web design finds limited effects of varying trust appeals and the amount offered in terms of perceptions of such emails, but a clear divergence in terms of recall about the offers. Last, I suggest the implications of this analysis for understanding both the scammer and scammed. More broadly, this analysis problematizes conventional views of such scams and suggests novel approaches to analyze existing data.

History and Evolution of the Scam

Although similar scams appear in the sixteenth century (Zuckoff 2005), the modern Nigerian AFF scam finds its roots in the late 1970s and early 1980s (Wizard 2000). With Nigeria's economic collapse of the 1980s, scammers relied primarily on stolen or counterfeit letterhead sent to primarily American and British businesses (Delio 2002).[2] As early as 1997, scammers mailed over three thousand offers a week, largely to the US and UK (US Department of State, 1997: 5). The proliferation of the scam in part correlates with shifts in Nigeria's political economy, with oil wealth creating a culture of corruption and political patronage. While initial letters were almost exclusively in English, increasingly scammers have translated letters into Spanish, Portuguese, and French among other languages.

The internet simply allowed for the proliferation of both scam letters and potential targets (see Smith 2006:1). The often butchered or antiquated Victorian-era English in such letters[3] may suggest small-time scammers at work. However, Nigeria's Interpol suggests that scammers were more likely to be professionals working as part of an organized hierarchy not unlike other forms of organized crime. For example, in Nigeria, the bottom rung collect email addresses and send the letters, often referred to as "Yahoo boys" because of the tendency to use free email services but also their age (usually ages 12 to 16). The next rung processes the replies. As one moves up the hierarchy, the average scammer is more educated. Furthermore, many scam networks are organized along ethnic or linguistic lines, especially in Nigeria, which not only facilitates coordination but complicates attempting to start a solo-operated scam.

Oyesanya (2004) claims the scam constitutes Nigeria's fifth largest source of income, leading even former U.S. Secretary of State Colin Powell to call Nigeria as "a nation of scammers" (Glickman 2005). Although the scam may have its origins in Nigeria, perpetrators

exist beyond West Africa. For example, Hong Kong police in March 1998 arrested 54 persons with over 13,000 letters about to be sent (Smith et al. 1999: 3). Cukier et al. (2007) find only 36 of the 202 active scam rings involved in advance free frauds were based out of Nigeria, with the UK (20) and Spain (18) also having similar active networks.[4] Long and Osofisan (2011) tracked the IP addresses of 400 randomly selected spam mails collected over a two year period, finding only 20.4% originated in Africa, with more from Europe (23.2%) and North America (28.5%). Costin et al. (ND) in their sample identified 63% of the phone numbers associated with 419 scams to Africa, with 31% from the UK.

While the origins differ among scammers, one broad goal unites them all: to convince another to part with their money.[5] The first email a potential dupe receives thus must include a narrative not only plausible to the recipient but which motivates the recipient to respond. Yet scammers face the challenge of finding those potentially naïve or greedy enough to relinquish their money and separating them from those who will not fall prey. Sending just to groups believed a priori to be gullible risks missing other potential dupes. Furthermore, scammers hope to avoid those who wish to waste the scammers' time without a payoff (Plumer 2012).[6] Scammers have limited information about their targets, often no more than an email address.[7] Nor is the distribution of would be victims known in any particular population. Thus scammers do not know if potential dupes are randomly distributed or densely packed into a particular geographical or demographic category.

Herley (2012) contends that these email scams are not simply blanket appeals, but their often poorly constructed English appeals intend to dupe respondents into viewing the writer as naïve and less intelligent (e.g. Peel 2006). An implausible offer further provides an efficient means to separate those potentially willing to hand over their money versus those that never

will.[8] Although few are immune to scams, [9] unsophisticated appeals greatly reduce the time necessary in generating new letters. Scammers attempt to maximize earnings through minimal efforts, relying increasingly on automated email harvesting and focusing the efforts on the scant few who respond. An implausible story in essence casts a very wide net but one with big holes.

This purported logic contrasts with that of Terrill Caplan, chief security office for Fraud Aid, who argues the email scams follow a separate strategy, attempting to appeal to one's sense of adventure through an exotic narrative.[10] Similarly appeals may play upon Westerners ignorance of Africa, what Smith (2009: 32) refers to as "sanctioned ignorance". Choosing Nigeria or a similar locale may be in part to appeal to a sense of adventure or exoticism, with rich narratives to induce an emotional appeal rather than rational behavior (Cukier et al. 2007). Ironically, the image of corruption throughout many African countries may benefit scammers in that the possibility of hidden fortunes seems more plausible in the region compared to stable democracies with greater forms of oversight. However, neither explanation explicitly addresses variation in appeals, with a general assumption that such variation is of little importance. Whereas some scammers use contemporary events to make their offers appear more plausible (Sullivan 2005; Zuckoff 2006), such tailoring remains largely superficial to the casual observer. Many such emails also have tracking codes at the bottom, evidence that scammers are testing which formats receive the greatest response and adjust their appeals accordingly, contrasting the image of a simple boilerplate strategy.[11]

Most estimates suggest at best a one percent response rate to AFF scam emails (Dyrud 2005). Longe and Osofisan (2011:20) claim the scam only needs to receive a hundred responses per ten million messages (0.001% success rate) to be profitable (also see Levy 2003). Cranor and LaMacchia (1998) found that Nigerian scam letters comprised 35% of unsolicited bulk mail in

their analysis, suggestive that scammers expect a low response rate. Interviews suggest that those on the bottom rung typical make only $1 a day, further suggesting the ease in turning a profit on this scam format.

The motivations of the recipient also require attention. The initial costs for collaboration pale in comparison to the promised windfall offered, providing a sense of rationality for the victim to continue as a scammer increases demands of fees, bribes, and associated hurdles. This may explain in part the size of the reward scammers claim. For example, Nhan et al. (2009) appears to be the only study that attempted to track the amount offered, finding only 10.9% of their sample offering $100,000 or less and 69.7% over $1,000,000.

Nigerian scam emails commonly appeal to both trust and greed and thus in this way operate differently than other email spam operations that focus on misleading web design or computer engineering more generally. The scam relies heavily on conveying a mutual relationship with increasing levels of trust, even while letters maintain design flaws, that potentially undermine trust (Tsow and Jakobsson ND). The narrative commonly includes references to trusting the recipient with their money, suggestive that the sender is taking a significant risk. While it may be difficult to identify the types of letters which ultimately are more effective in recruiting dupes, a focus on trust language and perceptions of trust provides a useful proxy.

Existing research also shows limited evidence of who is most susceptible to Nigerian email scams. Age may correlate with susceptibility as younger recipients, especially those more technologically savvy, theoretically should identify scams more easily, although Downs et al. (2006) found that those with less experience online were more suspicious of emails that were not personalized. The role of gender is unclear as well. The broader literature on risky online activity

and susceptibility to phishing efforts remains inconclusive (e.g. Milne et al. 2009; Hamburger and Ben-Artzi 2000; Hamburger and Ben-Artzi 2003). One also assumes that those with lower levels of education and household income would be more persuadable. For example, recipients unaware of the scam or who are struggling financially would be expected to be less cautious in interpreting a proposal that offers a solution to their financial woes. Yet to date, demographic correlates to this scam have not been empirically identified.

Research Design: How to Analyze Nigerian Scams

Analyzing Nigerian scams in a systematic way remains a daunting task on many levels. For example, few readily admit to being scammed. In addition, the US Federal Trade Commission collects scam emails, but does not make their collection available for research purposes. Scholars often attempt to collect the scam letters in some systematic way, such as those received over a set period of time in one's university email account (Cukier et al. 2007; Nhan et al. 2009; Onyebadi and Park 2012). This method remains problematic, as scammers increasingly use software to harvest email addresses from the web, a university email account's likelihood of receiving a scam letter most likely correlates with the frequency in which the address is posted online. Anecdotal evidence suggests that if one responds to a scam letter, they appear more likely to receive additional letters either from the same scammer posing as a different person or a different scammer altogether. Increasingly sophisticated spam filters also prevent many attempts from even reaching their intended audience. Other attempts to analyze the Nigerian scam remain underdeveloped. Glickman (2005) documents the responses he receives from interactions with scammers, but this too provides limited insight into broader trends within the scam framework. Efforts at interviewing or surveying the scammers also face logistical hurdles, including researchers potentially being labeled spammers themselves.

In contrast, I propose a mixed-method approach. First is a content analysis of existing scam emails. Social scientists have applied various means to decipher meaning from text (e.g. Berelson 1952; Holsti 1969) and computer assisted automated content analysis overcomes many of the concerns in human coding (.e.g. Benoit and Laver 2003; Laver et al. 2003). For the automated content analysis, this paper uses Wordstat software from Provalis.[12] Automated content analysis allows us to uncover patterns in text otherwise overlooked by the naked eye due to the sheer number of emails or synonyms that otherwise miss being properly coded. Scam emails were collected using a web crawler on the 419 scam email archives from www.419scam.org, a site dedicated to online scam prevention. This generated 540,219 email letters from 2004-2012, saved as individual files to be treated as the unit of analysis. This set more closely approximates the total population of such scam attempts than previous studies relying on at best a few hundred self-collected emails. Term frequencies within these emails produce the basis for initial empirical analysis.

To supplement the automated content analysis, I conducted an experiment embedded in a web survey, recruiting 242 American respondents from mTurk. Experimental work has increased in political science (e.g. Druckman et al. 2006; Barabas and Jerit 2010) and should provide distinct advantages to understanding the Nigerian email scam, while mTurk provides a cost-efficient means to test experimental designs on a broader population than college students. In particular, respondents can be randomly assigned variations of scam email templates to identify whether the content of the email influences perceptions and recall. Respondents are first asked a series of demographic questions to evaluate potential variation in susceptibility to email scams. Next respondents are randomly assigned to one of four templates in the style of an actual Nigerian email scam letter, including the attempts to appear more sophisticated while

maintaining grammar errors (see Blommaert and Omoniyi 2006). The intent here was to uncover perceptions of such scams and how respondents interpret the wording of letters by manipulating two aspects of the letter: references to trust and the amount of the offer. The length of all four emails is the same, 242 words. In terms of trust language, the first version makes no explicit references to trust, while the second makes nine explicit references (see Appendix). In terms of the monetary offer, the first version offers thirty percent of a supposed ten million dollars. This award amount—three million dollars—was chosen not only due to its general consistency with studies on the amounts offered in AFF appeals but also, unlike offers in the billions, may be viewed as more credible. The second version offers a much larger award, thirty percent of a hundred million dollars (thirty million dollars), an offer again consistent with AFF letters. For simplicity the letters do not mention their supposed place of origin, while identifying the writer as female (based on the name "Marie"). After reading the template, respondents are asked to rate perceptions of the letter on a five point scale and recall several facets of the letter. Afterwards, respondents are asked if they have received similar requests in the past as a means to evaluate whether previous exposure influences perceptions.

Content Analysis of Emails

Table 1 displays data on the percentage of emails which contain specific references. In terms of geographic region, 12.56% of the emails mentioned Nigeria (a total of 67,836 times), which contrasts with common perceptions of the scams yet consistent with previous empirical studies. African countries more broadly are referenced in 43.6% of emails (a total of 235,522 times), consistent with attempts to appeal to a sense of the exotic. Meanwhile European countries are referenced in 36.2% of cases (461,729 times). Despite the conventional wisdom regarding the

scam's connection to Nigeria, analysis of the scam letters shows claims of a broader geographical origin. Next, the size of the money available as part of the reward for cooperation is analyzed.[13] Here it is clear that offers of millions of dollars is the norm: 64.2% of emails reference at least one million dollars (a total of 542,825 times). In contrast, rewards in the thousands appear in less than a third of cases (29.94%) and a referenced 194,391 times. At the other end, offers of a billion dollars or more were rare, appearing on only 1.78% of emails and referenced a total of 10,843 times. Finally, a dictionary was created in WordStat to capture not only multiple variations of the word trust but also relevant synonyms.[14] A total of 825,500 references to trust were identified, with a majority of emails (60.91%) including at least one such reference, suggestive of the importance of trust within the scam narratve.

<Insert Table 1 Here>

To identify further the correlates of trust within the scam emails, Table 2 presents a crosstabulation of emails referencing trust and offers in the thousands, millions, or billions. For simplicity and because of the length of each email vary widely, I employ binary measures of each variable. Of particular note, across all three monetary offers, a supermajority included trust references, with higher offers more frequently including trust references. Since some emails may include multiple monetary references, Table 2 also includes whether any of the three offers were mentioned. Again, a supermajority includes trust references. In contrast, just under forty percent of emails with none of the monetary references include trust language. Table 2 similarly breaks down trust references and whether Nigeria or other African countries are mentioned. Supermajorities of emails referencing Nigeria also included trust language, with a slightly higher rate among other African countries. Meanwhile, a majority of emails that did not reference an African country (including Nigeria) included no reference to trust. Overall these results suggest

the need to appeal to trust, especially within the narrative of larger offers, within the exotic narrative.

<Insert Table 2 Here>

Experimental Survey Analysis

While we see clear patterns in the scam emails, it remains unclear how such variations are perceived by these targets. Experimental analysis allows us to identify whether marginally different appeals generate divergent responses. In my experimental web survey, respondents are first asked basic demographic questions. This is followed by random selection to one of four email prompts (see Appendix) that can be summarized as follows:

Letter A: No appeals to trust/ $3million offer
Letter B: Appeals to trust/ $3million offer
Letter C: No appeals to trust/ $30million offer
Letter D: Appeals to trust/ $30million offer

After reading a randomly assigned email template, respondents were asked the following statements on a five-point Likert scale (strongly disagree to strongly agree):

1. The author can be trusted
2. The author's monetary offer is appealing
3. I would likely respond to an email message like this one
4. There is no harm in responding to messages like these

Table 3 presents the percentage of respondents that agreed or strongly agreed with each of the four statement, broken down by the version of the letter received. First, less than a fifth of respondents stated that the author of the letter could be trusted, with no clear pattern based on the trust references in the letters, suggestive of the difficulties scammers face in finding dupes.

Secondly, a majority of respondents across all four letters acknowledged that the offer was appealing. Third, only a fraction of respondents claimed that they were likely to respond to letters like these, with higher rates among those loaded with trust references. The divergence is most clear between Letters A & B, both which offer a three million dollar award. Finally, a small minority of respondents saw no harm in responding to such offers, with slightly higher rates among those who received letters with explicit references to trust. However, if using Letter A as the baseline, few of the distributions of responses between Letter A and the other three letters reach statistical significance, with the main distinction between Letter A and Letter C where only the amount of the award differed, suggesting the limited salience in trust references. Here trust in the author and perceptions in harm were significant at .10 and the likelihood of responding significant at .05.

<Insert Table 3 Here>

Respondents were also asked about their recall from the letters, first asked to remember the amount offered in the letter, either in the exact amount or the percentage, and then the gender of the author (simply addressed as Marie in the letter). Table 4 presents the percentage of respondents who correctly identified the amount offered in the letter and the gender of the author. While supermajorities across each letter type correctly identified the amount the author offered, this was consistently higher among the letters without trust references. In the three million dollar letters, only 73.02% of respondents who received the trust-laden letters remembered the monetary offer, compared to 89.87% without explicit trust references, statistically significant at .01. A similar but less pronounced pattern is seen with the thirty million dollar letters: 75.56% of respondents who received the trust letter correctly identified the monetary offer compared to

81.48% who received no explicit trust references. In contrast, little variation is seen between letter types in regards to identifying the author as female. These initial findings seem to suggest that increased references to trust negatively influence a respondent's ability to recall the amount offered.

<Insert Table 4 Here>

To further identify whether subtle differences in the letters shift perceptions, Tables 5 and 6 present a series of ordinal logit models on each of the four perceptions mentioned above on a five point Likert Scale ranging from strongly disagree to strongly agree. Two specifications are tested. The first just includes controls for Letters B-D leaving Letter A as the base category. The second includes controls for gender, age, and education, as well as a measure of risk aversion based on a five-point Likert scale reponse (strongly disagree to strongly agree) to "I am risk averse", and a dummy variable for those respondents who claimed to have never received an email similar to the one presented.

Across the models, little variation is seen based on the type of letters. In terms of trust, all three letters positively correlate with trust, but only Letter C, with the offer of $30 million and no references of trust, reaches even the .10 level of significance in both models. In terms of finding the offer appealing, Letter B negatively correlates at the .10 level. In addition, Letters B-D all positively correlate with the likelihood to respond, yet Letter C again is the only version significant at .10 or greater in both models, while the version is also weakly significant in the base model regarding that responding would be no harm. Lastly, all three versions positively correlate with believing that responding to such a letter as harmless, but none reach significance in the expanded model. In terms of controls, unsurprisingly education negatively correlates with

perceptions in all four models, significant at .05 or stronger. Furthermore, those that stated they had never received an email like the presented template positively correlates with perceptions at .01 or stronger and with the largest coefficient of any variable. Overall the results suggest that appeals to trust and the size of the award have only minimal influence at best on public perceptions, while exposure to such offers in the past greatly reduces one's perceptions. Unfortunately the survey does not ask additional questions regarding this past experience to identify when one responded to such an offer in the past or when they received such an email. The findings do suggest that rather than attempt to lure dupes through confidence building language or larger monetary offers, scammers should simply attempt to find those who have not received such offers before, consistent with Herley's (2012) claims.

<Insert Table 5 Here>
<Insert Table 6 Here>

Whereas perceptions appear marginally influenced by references to trust or the amount offered, a clearer pattern emerges when shifting to recall. Table 7 presents the results of two binary logit models with the dependent variable of correctly identifying the monetary award offered, again using Letters B through D as the main independent variables with an extended model including the same controls as the previous ordinal logit models. In both models the letters highlighting trust (B and D) negatively correlate with correctly remembering the award amount, significant at .05. Meanwhile, education and experience seeing similar letters had no effect in the extended model. In addition, females were less likely to correctly identify while the risk averse were more likely, significant at .05.

Predicted probabilities of the extended models holding the controls at their mean and only altering which version of text the respondent receives further highlights this distinction. In

both trust-referencing versions (Letter B and D), the predicted probability of correctly identifying the monetary offer were identical (76 percent), compared to 84 percent for Letter C and 91 percent for Letter A. These findings suggest that trust building rhetoric potentially distracts the reader away from the amount offered, but the causal mechanism here remains unclear. If trust wording encouraged confidence building, readers may simply be focusing on assistance in the abstract more than the amount. However, the earlier findings seem to suggest trust rhetoric does not have its desired influence. Thus, this pattern may be the result of such wording leading readers to pay less attention overall, dismissing the offer outright.

<Insert Table 7 Here>

Conclusion

This analysis identifies patterns in the letters of actual email scams and the perceptions of similarly worded letters through an experimental web design. This multi-method approach attempts to tackle areas of the Nigerian email scam often overlooked, in part because of assumptions that the emails themselves provide marginal insight into the scammers and the scammed. Admittedly this is preliminary research in that the forms of such scam emails vary considerably and that this analysis focuses solely on the initial contact. However, the results here suggest that both that scam letters implicitly contain trust rhetoric to appeal to their potential dupes, but that such tailoring does not necessarily benefit the scammer. In other words, scammers may be better off with generic blanket appeals and attempting to nab only the most gullible.

Future work may further unpack the common variations within such email scams, such as directly measuring versions reported from different countries or whether the gender of the supposed author influences perceptions. Similarly, while scammers have increased appeals based on religious commonalities, no study has directly tackled whether such appeals benefit the scammers. A broader question on how to undermine the effectiveness of the Nigerian email scam also remains. While the success rate of the scam remains low, the losses are non-negligible. The findings here suggest that those who had not previously received such email requests generally had more positive views of the email. Although efforts at public awareness may help, a more fruitful approach may be to use automated content analysis as a means to construct better spam filters, identify patterns beyond the country of origin and the large monetary awards by focusing on their combination with trust rhetoric.

REFERENCES

Babad, E. & Katz, Y. (1991). Wishful thinking—against all odds. *Journal of Applied Social Psychology,* 21(23), 1921–1938.

Barabas, J. & Jerit, J. (2010). Are survey experiments externally valid? *American Political Science Review,* 104(2), 226-242.

Barron, A. (2006). Understanding spam: a macro-textual analysis. *Journal of Pragmatics,* 38(6), 880–904.

BBC. (2004). Huge Nigeria scam trial collapses. July 20. http://news.bbc.co.uk/2/hi/africa/3909233.stm.

Benoit, K. & Laver, M. (2003). Estimating Irish party policy positions using computer Wordscoring: the 2002 election –a research note. *Irish Political Studies,* 18(1), 97-107.

Bergiel, B.J., Bergiel, E.B. & Balsmeier, P.W. (2008). Internet cross border crime: a growing problem. *Journal of Website Promotion,* 3(3/4), 133-142.

Blommaert, J. & Omoniyi, T. (2006). Email fraud: language, technology, and the indexicals of globalization. *Social Semiotics,* 16(4), 573-605.

Brooks, G. (1994). Outmaneuvered: how a recurring scam cost an accountant and his wife $54,000. *Wall Street Journal.* June 24. Pg. A1, A6.

Buse, U. (2005). Spam scams: Africa's city of cyber gangsters. *Spiegel Online International.* November 7. http://www.spiegel.de/international/spiegel/spam-scams-africa-s-city-of-cyber-gangsters-a-384317.html

Cheng, J. (2010). Suckers victims lost $9.3 billion to 419 scammers in 2009. Arstechnica. January 29. Available at: http://arstechnica.com/security/2010/01/victims-lost-93-billion-to-419-scammers-in-2009/

Costin, A., Isacenkova, J., Balduzzi, M., Francillon, A. & Balzarotti, D. ND. The role of phone numbers in understanding cyber-crime schemes. http://www.iseclab.org/people/embyte/papers/phonyphones.pdf

Cranor, L.F. & LaMacchia, B.A. (1998). Spam! *Communications of the ACM,* 41(8), 74-83.

Cruickshank, D. (2001). I crave your distinguished indulgence (and all your cash). Salon.com 7 August http://www.salon.com/2001/08/07/419scams/

Cukier, W.L., Nesselroth, E.J. & Cody, S. (2007). Genre, narrative and the 'Nigerian letter' in electronic mail. Proceedings of the 40th Hawaii International Conference on System Sciences. http://csdl2.computer.org/comp/proceedings/hicss/2007/2755/00/27550070a.pdf

Delio, M. (2002). Meet the Nigerian e-mail grifters. *Wired News*. July 12. http://www.wired.com/culture/lifestyle/news/2002/07/53818?currentPage=all

Downs, J.S., Holbrook, M.B. & Cranor, L.F.. (2006). Decision strategies and susceptibility to phishing. Carnegie Mellon University Research Showcase. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1026&context=isr&sei-redir=1&referer=http%3A%2F%2Fscholar.google.com%2Fscholar%3Fstart%3D20%26q%3D%2522experiment%2522%2Band%2BNigerian%2Bemail%2Bscam%26hl%3Den%26as_sdt%3D0%2C18#search=%22experiment%20Nigerian%20email%20scam%22

Druckman, J.N., Green, D.P., Kuklinski, J.H. & Lupia, A. (2006). The growth and development of experimental research in political science. *American Political Science Review,* 100(4), 627-635.

Dyrud, M.A. (2005). I brought you a good news: an analysis of Nigerian 419 Letters. Paper presented at the Association for Business Communication Annual Conference, Irvine, California. http://www.businesscommunication.org/.conventions/Proceedings/2005/PDFs/07ABC05.pdf

FraudAid. (ND). Nigerian scam letters: sent out by the thousands. Fraudaid.com http://fraudaid.com/ScamSpeak/Nigerian/419_Hidden_Facts/emails_sent_out_by_the_thousands.htm

Glickman, H. (2005). The Nigerian '419' advance fee scams: prank or peril? *Canadian Journal of African Studies,* 39(3), 460-489.

Haines, L. (2004). Nigerian judge claims 'no jurisdiction to hear it. *The A Register*. July 20. http://www.theregister.co.uk/2004/07/20/419_trail_collapse/

Hamburger, Y.A.& Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the internet." *Computers in Human Behavior,* 16(4), 441-449

Hamburger, Y.A.& Ben-Artzi, E. (2003). Loneliness and internet use. *Computers in Human Behavior,* 19(1),71 – 80.

Herley, C. (2012). Why do Nigerian scammers say they are from Nigeria? Unpublished paper. Available at: http://research.microsoft.com/pubs/167719/whyfromnigeria.pdf

Kahneman, D. & Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Econometrica,* 47(2), 263–291.

Krebs, B. (2011). Where did that scammer get your email address? Krebs on Security blog. April 25. http://krebsonsecurity.com/2011/04/where-did-that-scammer-get-your-email-address/

Kuhnen, C.M.& Knutson, B. (2005). The neural basis of financial risk taking. *Neuron,* 47(5), 763–770.

Laver, M., Benoit, K. & Garry, J. (2003). Extracting policy positions from political texts using words as data. *American Political Science Review,* 97(2), 311-331.

Lazarus, D. (2003). Greed fuels big internet scam. San Francisco Chronicle 12 January: Gl <http://web.lexis-nexis.com/universe/docu ment?_m=8df4b2e3b65c89c6ef74c4537c0ca34c> accessed 23 May 2003.

Legard, D. (2003). E-mail threats increase sharply. *PC World*. http://www.pcworld.com/article/107930/article.html

Levy, E. (2003). Crossover: online pests plaguing the offline world. *IEEE Security & Privacy,* 1(6), 71-73.

Longe, O.B., Mbarika, V. , Kourouma, M., Wada, F & Isabalija, R. (2009). Seeing beyond the surface: understanding and tracking fraudulent cyber activities. *International Journal of Computer Science and Information Security,* 6(3), 124-135. http://arxiv.org/ftp/arxiv/papers/1001/1001.1993.pdf

Longe, O. & Osofisan, A. (2011). On the origins of advance free fraud electronic emails: a technical investigation using internet protocol address tracers. *African Journal of Information Systems,* 3(1), 17-26.

Milne, G.R., Labrecque, L.I. & Cromer, C. (2009). Toward an understanding of the online consumer risky behavior and protection practices. *Journal of Consumer Affairs,* 43(3), 449-473.

Nhan, J., Kinkade, P. & Burns, R. (2009). Finding a pot of gold at the end of an internet rainbow: further examination of fraudulent email solicitation. *International journal of Cyber Criminology,* 3(1), 452-475.

Onyebadi, U. & Park, J. (2012). 'I'm Sister Maria, please help me': a lexical study of 4-1-9 international advance fee fraud email communications. *International Communication Gazette*, 74(2), 181-199.

Oyesanya, F. (2004). Nigerian internet 419 on the loose. Nigeria Village Square. March 28. http://nigeriavillagesquare.com/articles/femi-oyesanya/nigerian-internet-419-on-the-loose-13.html

Peel, M. (2006) Nigeria-related financial crime and its links with Britain. Available at: www.chathamhouse.org.uk/files/3377_nigeria1106.pdf (accessed 24 December 2010).

Plumer, B. (2012). Why Nigerian email scams are so crude and obvious. *Washington Post* Wonkblog. June 22. Available at: http://www.washingtonpost.com/blogs/wonkblog/wp/2012/06/22/why-nigerian-e-mail-scams-are-so-crude-and-obvious/

Rosato, D. (2006) Hello, sucker. *Money,* 35(11), 112–121.

Rosenbaum, R. (2007). How to trick and online scammer into carving a computer out of wood. *The Atlantic*. June. http://www.theatlantic.com/magazine/archive/2007/06/how-to-trick-an-online-scammer-into-carving-a-computer-out-of-wood/305903/

Schiesel, S. (2004). Turning the tables on e-mail swindlers. New York Times 17 June: Gl, G7.

Shefrin, H. & Statman, M. (1985). The disposition to sell winners too early and ride losers too long: theory and evidence. *Journal of Finance,* 40(3), 777-790.

Simon, H.A. (1956). Rational choice and the structure of the environment. *Psychological Review,* 63,129–138.

Smith, A. (2009). Nigerian scam e-mails and the charms of capital. *Cultural Studies,* 23(1), 27-47.

Smith, D.J. (2006). *A culture of corruption: everyday deception and popular discontent in Nigeria*. Princeton: Princeton University Press.

Sullivan, B. (2005). 'Nigerian scams' keep evolving. MSNBC News. June 10. Available at: http://www.msnbc.msn.com/id/8171053/ns/technology_and_science-security/t/nigerian-scams-keep-evolving/#.ULV4t4bm4uc

Thaler, R. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior and Organization,* 1: 39-60.

Tsow, A. & Jakobsson, M. (ND). Deceit and deception: a large user study of phishing. Working Paper. ftp://ftp.cs.indiana.edu/pub/techreports/TR649.pdf

Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty: heuristics and biases. *Science,* 185(4157), 1124–1131.

US Department of State. (1997). Nigerian Advance fee fraud.

United States Secret Service. (2002). Public awareness advisory regarding "4-1-9" and "advanced free fraud" schemes. http://secretservice.gov/alert419.shmtl

Viosca, C., Bergiel, B.J. & Balsmeier, P**. (**2004). Effects of the electronic money fraud on the brand equity of Nigeria and Africa. *Management Research News,* 27(6), 11-20.

Wizard, B. (2000). *Nigeria 419 scam: game over*. Wallowa, Oregon: Starguill International.

Zuckoff, M. (2005). Annals of crime: the perfect mark. *The New Yorker,* 82(13), 36-42.

Zuckoff, M. (2006). The perfect mark: how Massachusetts psychotherapist fell for a Nigerian email scam. *The New Yorker*. May 15. http://www.newyorker.com/fact/content/articles/060515fafact

Appendix[15]

Letter A (no appeals to trust/$3 million offer)
Permit me to introduce myself and my situation. I think you are the type of person I can do business. By matter of this expectation I must not hesitate to discuss with you this proposal. Before the death of my father he left me a sum of over US$10,000,000 (ten million dollars) kept in a private bank. Presently, I am in hospital where I have been undergoing treatment for cancer, where my doctor told me that I would not last for the next three months. Because my relatives and friends plundered so much of my father's wealth since my illness, I cannot live with the agony of leaving this huge responsibility to any of them. I am worried that those with dishonest intentions will get access to this money when I die.

I humbly request that you follow my instructions closely. I also indulge you not to make undo use of the information given to you. I request that you will not tell others about this business for I fear their insincere purposes. I am seeking your assistance to receive this money into a safe account in your country and to provide good investment plans and distribute the money to charity organizations. For your cooperation and assistance I am willing to offer you 30% of the total sum (three million dollars) as compensation for your effort after the successful transfer of these funds to the US.

Your assistance is very appreciated,
Marie

Letter B (appeals to trust/$3 million offer)
Permit me to introduce myself and my situation. I believe you are a honest and trustworthy person I can do business. By matter of trust I must not hesitate to confide in you this proposal. Before the death of my father he left me a sum of over US$10,000,000 (ten million dollars) kept in a private bank. Presently, I am in hospital where I have been undergoing treatment for cancer, where my doctor told me that I would not last for the next three months. Because my relatives and friends plundered so much of my father's wealth since my illness, I cannot live with the agony of entrusting this huge responsibility to any of them. I am worried that those with dishonest intentions will get access to this money when I die.

I humbly request that you follow my instructions closely. I also indulge you not to make undo use of the information given to you. I trust that you will not tell others about this business for I fear their insincere purposes. I am relying your assistance to receive this money into a safe account in your country and to provide good investment plans and distribute the money to charity organizations. For your trust and assistance I am willing to offer you 30% of the total sum (three million dollars) as compensation for your effort after the successful transfer of these funds to the US.

Your trust is very appreciated,
Marie

Letter C (no appeals to trust/$30 million offer)
Permit me to introduce myself and my situation. I think you are the type of person I can do business. By matter of this expectation I must not hesitate to discuss with you this proposal. Before the death of my father he left me a sum of over US$100,000,000 (hundred million dollars) kept in a private bank. Presently, I am in hospital where I have been undergoing treatment for cancer, where my doctor told me that I would not last for the next three months. Because my relatives and friends plundered so much of my father's wealth since my illness, I cannot live with the agony of leaving this huge responsibility to any of them. I am worried that those with dishonest intentions will get access to this money when I die.

I humbly request that you follow my instructions closely. I also indulge you not to make undo use of the information given to you. I request that you will not tell others about this business for I fear their insincere purposes. I am seeking your assistance to receive this money into a safe account in your country and to provide good investment plans and distribute the money to charity organizations. For your cooperation and assistance I am willing to offer you 30% of the total sum (thirty million dollars) as compensation for your effort after the successful transfer of these funds to the US.

Your assistance is very appreciated,
Marie

Letter D (appeals to trust/$30 million offer)
Permit me to introduce myself and my situation. I believe you are a honest and trustworthy person I can do business. By matter of trust I must not hesitate to confide in you this proposal. Before the death of my father he left me a sum of over US$100,000,000 (hundred million dollars) kept in a private bank. Presently, I am in hospital where I have been undergoing treatment for cancer, where my doctor told me that I would not last for the next three months. Because my relatives and friends plundered so much of my father's wealth since my illness, I cannot live with the agony of entrusting this huge responsibility to any of them. I am worried that those with dishonest intentions will get access to this money when I die.

I humbly request that you follow my instructions closely. I also indulge you not to make undo use of the information given to you. I trust that you will not tell others about this business for I fear their insincere purposes. I am relying your assistance to receive this money into a safe account in your country and to provide good investment plans and distribute the money to charity organizations. For your trust and assistance I am willing to offer you 30% of the total sum (thirty million dollars) as compensation for your effort after the successful transfer of these funds to the US.

Your trust is very appreciated,
Marie

Table 1: Percentage of Emails Containing Selected References

Regions		**Reward**		**Trust**	
Nigeria	12.56	Thousand	29.94	Trust	60.91
Africa	43.6	Million	64.20		
		Billion	1.78		

Table 2: Crosstabulations of Trust References to Monetary Offers and Locale

	With Trust	**Without Trust**	**N**
Monetary Offers			
Thousand	68.14	31.86	161723
Million	72.74	27.26	346810
Billion	85.3	14.7	9600
Any of the Three	70.53	29.47	373375
None of the Three	39.36	60.64	166844
Locale			
Nigeria	72.19	27.81	67836
Africa	75.36	24.64	235522
Either	74.59	25.41	283609
Neither	45.78	54.22	256610
Monetary and Locale			
References Both	77.67	22.33	226333
References Neither	27.31	72.69	109568

Table 3: Summary Statistics of Positive Evaluations Based on Letter Template

	A (3 million)	B (3 million/trust)	C (30 million)	D (30 million/trust)
Author can be trusted	10.12	17.46	18.52	8.69
Offer is appealing	50.64	50.80	57.40	52.18
Likely to respond	3.80	12.69	7.41	8.69
No harm in responding	7.59	11.11	3.70	4.35

Table 4: Rate of Correctly Identifying Aspects of the Letter Templates

	A (3 million)	B (3 million/trust)	C (30 million)	D (30 million/trust)
Correct amount identified	89.87	73.02	81.48	75.56
Correct gender identified	86.08	90.48	85.19	84.44

Table 5: Ordinal Logit Models Based on the Perceptions of the Model (Can Be Trusted and Offer Appealing)

	Can Be Trusted		Can Be Trusted		Offer Appealing		Offer Appealing	
	Coeff	SE	Coeff	SE	Coeff	SE	Coeff	SE
Letter B (3 million/trust)	0.55t	0.33	0.43	0.35	-0.28	0.31	-0.60t	0.32
Letter C (30 million)	0.61t	0.34	0.61t	0.37	0.20	0.32	0.11	0.33
Letter D (30 million/trust)	0.12	0.37	0.29	0.39	0.07	0.34	0.00	0.35
Female			-0.14	0.27			-0.57*	0.25
Age			-0.01	0.01			-0.04***	0.01
Education			-0.29**	0.10			-0.28**	0.09
Risk adverse			-0.14	0.14			0.08	0.13
Never similar email			1.86***	0.29			0.85**	0.27
N	242		241		242		241	
Pseudo R^2	0.01		0.11		0.00		0.07	

[t] p<.10; * p<.05; **p<.01; ***p<.001

Table 6: Ordinal Logit Models Based on the Perceptions of the Model (Likely to Respond and No Harm)

	Likely to Respond		Likely to Respond		No Harm		No Harm	
	Coeff	SE	Coeff	SE	Coeff	SE	Coeff	SE
Letter B (3 million/trust)	0.73t	0.38	0.69	0.42	0.42	0.36	0.26	0.38
Letter C (30 million)	0.76*	0.39	0.76t	0.44	0.65t	0.36	0.55	0.39
Letter D (30 million/trust)	0.21	0.44	0.45	0.49	0.01	0.41	0.09	0.44
Female			0.18	0.33			0.17	0.29
Age			-0.02	0.02			-0.02	0.01
Education			-0.25*	0.12			-0.18	0.11
Risk adverse			-0.32t	0.17			-0.18	0.15
Never similar email			2.46***	0.34			1.70***	0.30
N	242		241		242		241	
Pseudo R^2	0.01		0.18		0.01		0.10	

[t] p<.10; * p<.05; **p<.01; ***p<.001

Table 7: Logistics Regression on Correctly Identifying the Monetary Award Offered

	Basic Model		Extended Model	
	Coeff	SE	Coeff	SE
Letter B (3 million/trust)	-1.19*	0.47	-1.12*	0.48
Letter C (30 million)	-0.70	0.51	-0.63	0.53
Letter D (30 million/trust)	-1.05*	0.51	-1.10*	0.52
Female			-0.85*	0.35
Age			0.00	0.02
Education			0.04	0.14
Risk adverse			0.45*	0.19
Never similar email			-0.10	0.39
Constant	2.18	0.37	1.08	1.05
N	241		241	
Pseudo R^2	0.03		0.08	

[t] p<.10; * p<.05; **p<.01; ***p<.001

[1] One victim, Frieda Springer-Beck of Germany, agreed to an out-of-court settlement with accused Nigerian scammer Fred Ajudua in 2005, but such cases remain rare (see Buse 2005).
[2] Handwritten notes using counterfeit postage stamps were also not uncommon still in the 1990s (Smith etl al (1999: 2).
[3] Cruickshank (2001) refers to writing style "as awkward and archaic as it is enchanting."
[4] Interviews with experts suggested that while a majority of AFF scams originated in Nigeria, cases were also common out of the Netherlands, France, South Africa, Germany, the UK, Benin, and Cote d'Ivoire.
[5] For example, Glickman (2005) suggests one motivation is compensation for slavery and colonialism.
[6] Scam baiting websites such as 419 Eater (http://www.419eater.com/) catalog just such efforts to waste the time and resources of scammers (also see Rosenbaum 2007).
[7] While various means are available to harvest email addresses, several companies also sell country specific email lists as well as email host specific lists. Several million email addresses can be purchased for under $500 (see Krebs 2011).
[8] As Herley (2012: 11) states, "since gullibility is unobservable, the best strategy is to get those who possess this quality to self-identify."
[9] One of the largest Nigerian scam payouts totaled $242 million, paid out by Nelson Sakaguchi, a director of Banco Noroeste Brazil (Haines 2004; BBC 2004). Surprising to none, the bank later filed for bankruptcy.
[10] Interview with Terrill Caplan on February 13, 2013.
[11] Interview with Terrill Caplan, February 13, 2013.
[12] See http://provalisresearch.com/products/content-analysis-software/wordstat-features/
[13] This measure admittedly does not distinguish between references to the amount the dupe will reportedly receive of the total amount of money claimed in the email.
[14] A list of the terms included in the dictionary is available by request.
[15] Trust references and the monetary offer are underlined for convenience but were not underlined in the web survey.