The Nigerian "419" Advance Fee Scams: Prank or Peril?

Harvey Glickman*

Introduction: "Why Worry?"

"[Nigeria]…a nation of scammers" (Colin Powell) [1]

"419 scams" ("four-one-nines" -- named after the numbered provision in the Nigerian Criminal Code against impersonating officials for financial gain) are e-mails and letters that reveal a very large sum of money stuck in an African (usually Nigerian, but lately in other West African countries) bank account or safety deposit location. In their present form, they originate with e-mails to all sorts of people, usually from business and academic lists, claiming that millions of dollars reside in an overlooked account for shipment of some goods into or out of an African country. The sender asks for a person's help in transferring the money to a legitimate bank account outside Africa and will share a percentage of the frozen funds with the recipient of the message. The owner of the account is invariably dead. The offer is to share the millions with the unsuspecting e-mail recipient if the recipient will send his/her bank account number, and perhaps later some earnest money, ostensibly to facilitate the eventual transfer.

These scams have flowered in the past thirty years, and while most everybody now ignores them, they have trapped an occasional minor celebrity,

e.g., Ed Mezvinsky, former U.S. Congressman from Kansas, now in jail for looting his mother-in-law's account (Brady 2003, 13; NBC 10 News 2003). This paper inquires into the nature of the 419 scams, and investigates why they persist in the face of what appears to be universal disdain. We attempt to discern their processes, their reach, and their significance for Africans and relations with Africa. (As illegal activity, perhaps similar to Mafia enterprises, it is difficult to say we are ever able to uncover all the facts.) Examples will be offered of typical scams run today. Who are the 419ers? How are 419 rings organized? Why do seemingly ordinary people fall for these schemes? Why have they apparently originated in Nigeria? Why does Africa continue to play such an important role as putative point of origin? What actions are being taken to reduce the spread? Is the danger limited to the gullible or are bigger stakes at play?

Legitimate Nigerian business people, already affected by drug traffic through the country, encounter difficulty in transacting their affairs. African, especially Nigerian, politicians, who are tainted by corruption, are also suspect scammers when they attempt to attract legal investment to African countries. Influential academic commentators place the 419 scams in the context of a growing "criminalization of the African state." (Bayart, Jean-Francois, Stephen Ellis, Beatrice Hibou 1999a, 104-106.)

More broadly, in terms of relations between Africa and Europe/North America, 419 scams may be the reversal of contemporary collaboration to essentially loot African resources by opportunistic Westerners and corrupt local officials.[2] Going even further, these scams may reflect peculiar social and cultural trends that undermines the growth of markets and legitimate institutions in circumstances of severe economic and social change (Bayart 1999, 114-116, Hibou 1999, 70-113). One informed observer argues that 419 scams reflect deap-seated and damaging cultural forces,

> a dislocation of value:…Based on cultural idioms of money magic, whereby human blood and body parts are stolen and used to conjure illicit wealth, the 419 represents nefarious trade, draining victims of their goods and cash through forged documents and staged performances. .. the 419 has migrated to the internet, where it has proliferated and shifted through digital "cloning" from the circuits of oil to the information highway… [a] return to tropes of hidden bullion taken out of circulation and buried beneath the ground. (Apter 2003)

Dimensions of the Present Analysis

We address the 419 scams at four levels of analysis:

On the surface, these cascading e-mails amuse most of us and sometimes attract the unwary into Ponzi-type schemes. Such schemes have bilked thousands

of people over hundreds of years. They are the "noise" and the nefarious excess of expanding commercial capitalism, today the flotsam of global marketeering. One examiner, perhaps a stand-in for some -- rather patronizing -- recipients, comments on the idiomatic language and range of human failings exposed, observing that some people may even be attracted by a lyrical "prose style that is as awkward and archaic as it is enchanting" (Cruickshank 2001). A few playfully adventurous internetters have turned "counterscammers," engaging in extended correspondence in games of revenge or entrapment.

On a second level, that of law and order, of fraud and victims, the 419s attract a combination of the curious, the naïve, and the sympathetic, into a vortex of ill fortune and money loss that sometimes is life threatening. The schemes today exploit greed and insouciance that capitalize on the news of human dislocation and civil war. On this level the schemes are viewed as a problem in racketeering and the need to crack African, and indeed global, crime syndicates (see MacDougall and Lamkin 1994, Bureau of International Narcotics and Law Enforcement Affairs 1997, Smith, Holmes and Kaufman 1999, Bi-National Working Group 2003, Canadian Press Service 2003, Nigeria Fraud 2003).

At a third, and indeed a social science level, 419 schemes are reflections of cultural and social dysfunctionality. On the one hand, they can be described as part of the now familiar excesses accompanying the drastic and rapid alteration of

economic systems, exemplified by Russia in the past two decades. Since independence in 1960, the Nigerian economy, for example, has passed through at least three major development phases – attempt at balanced growth, foreign assisted industrialization, and petroleum financed "Dutch disease" distortions (Wright 1998). On the other hand, 419 schemes reflect a political and cultural success syndrome, revolving around wealth, corruption, political patronage, and even elements of witchcraft that make for "Big Man" leadership (Wright 1998, Price 1975). Several observers have subsumed 419 schemes within the progression of politically supported corruption to an African criminal state: "from kleptocracy to the felonious state [?]" (Bayart 1999b, 1-31). This approach raises broad issues of development and political legitimacy.

Finally, at a fourth level, reflecting the global policy implication of the three previous levels, is a shadowy link to drug and arms traffic. In the post 9/11 world, who can predict what links might materialize to cash and small arms to warlords and terrorists? At this level, exposing and combating 419s becomes a tertiary element in a global police effort, affecting us all.

Anatomy of 419 "Come-ons"

Persons who actually take the time to read these e-mails would observe that initial contacts trade on contemporary events, but always appeal to greed in rehearsing a variation on a familiar tall tale. Nevertheless a uniform thread

infiltrates these solicitations. Perpetrators seek to forge a bond beyond greed between themselves and the reader, recently reflected in the vocabulary of piety and pity. Details of recent real events are provided. Most egregiously, in 2000, a number of 419 scam letters used the actual names of victims in the crash of the Kenya Airways A310, including links to news websites (Catan and Peel 2003, 21). Some part of the initial allure of the stories may be in the poor grammar and awkward word choice and phrasing. While it may seem strange to enter into a multi-million dollar transaction with someone who communicates obliquely, in fact scammers are playing upon a racist stereotype: that Africans are childlike, intellectually unsophisticated, innocent in business ways, and probably corrupt. In their latest incarnation scams play upon the readers' heartstrings -- a whole family has been tragically killed. Even the clichés of honor, pity, and secrecy seem part of a deliberate attempt to lure the unsuspecting recipient into a false belief that the sender is desperate as well as naïve.

To deal systematically with all four suggested dimensions of analysis, ideally we would need to spend some time in the field – Nigeria and, lately, South Africa -- perhaps as a participant-observer in the society of scammers. Although the writer has logged considerable time in Africa, Nigeria is not part of that field experience. As we will see, few victims ever actually meet their partners, without injury or worse. Interviewing scammers resembles infiltrating the Mafia, not part

of the training of social scientists. The preliminary analysis here is based on 294 e-mails collected in eight months of 2003. (Our total collection has swelled to 376 in mid-2004 and continues to grow.)[3] To characterize them within this brief period, our scam examples oscillated between sob stories and brisk business proposals. Curiously, within this sample and time period, dollar amounts seem to have decreased, perhaps a parallel move toward the realism of connecting to current events or an attempt to reach more ordinary people who cannot afford big figure sums. Claiming to be the relative of a late African political figure remains a popular choice. But other well-known political figures have been invoked. Three years ago a police officer responded to an e-mail, supposedly from the wife of the late former president, Joseph Estrada, in the Philippines. He was asked to meet several Filipinos in London: "they" turned out to be a lone African (Stephen 2001). Purely African stories and obviously African names may now raise suspicions. Recently, scammers have claimed to be relatives of 9/11 victims or former Iraqi officials (Lin-Fisher 2002, New Scientist 2003). Scammers have also ventured into domestic U.S. affairs. One scammer said he was a stock broker under investigation by the U.S. Internal Revenue Service; he needed your help to get at his millions in frozen assets. Another claimed to be inside the U.S. government, saying they had over-invoiced companies for taxes on dividends, stating "We wish to reimburse these payments to the accounts of trustworthy,

wealthy retirees like yourself." He offered reimbursement of your proportional entitlement of $396 billion over ten years (Hill 2003, 25). An interesting variation in the U.S.A. is for touring Africans to offer to buy a property on the spot for cash, if the property owner would help " clean" a suitcase of $ 3 million of smuggled currency (Slobodzian 2004, B3).

Among our received solicitations, as an empirical foray, we chose six deemed typical of spelling and punctuation. We replied to five (full texts contained in a separate document, author's Appendix Two, available as noted), in order to elicit a path toward some sort of transaction. The first one, from a "Mrs. M. Sese seko," exhibits several ubiquitous features. It is written in broken but understandable English, probably designed to elicit a condescending response, perhaps sympathy, perhaps confidence in the naivete of the sender. It stays close to actual facts about President Mobutu, his foreign mansions and his stashed loot outside the Congo. It comes from a woman, which is relatively new in scam history, possibly to elicit kindness as well as display vulnerability. Subsequently, we were handed off to a "son," Dennis Kongolo, mentioned in the initial e-mail, with whom we corresponded.

A second contact, also supposedly from a woman, also claimed a relationship to a real person recently killed, and went further in asking for help for several reasons, including furthering her education. (Due to a mix-up of *noms de*

plumes, we did not reply to this one.) It attempted to convince us that we are participating in an act of charity, in addition to receiving a commission for a business deal. The sum of $ 8 million was offered, maybe more believable than a larger figure, although the percentage of 30 per cent seemed designed to attract high rollers. It asked for no concrete information from the investor at the start. While this seems to waste time in applying a hook, it reflects an application of a learning curve; a personal bond is helpful.

A third communication hinted at bank scam. It contains more than usual obvious misspellings, again perhaps to instill a sense of superiority in the recipient; it purports to come from a manager of a bank (nonexistent as far as we could tell) in Benin, it trades on news of an airplane crash – not an infrequent event in Africa – and it boldly asks for a bank account and other personal information straightaway, referring to the legal formality of an "application as next of kin."

A fourth radiated clandestinity, as it is from an admitted corrupt official, who has come across a large amount of money that can be discretely siphoned out of the country. He seems either foolish or bold enough to give you 20 per cent or about $ 7 million for your assistance. The Nigerian National Petroleum Corporation is the national oil agency. The company name creates some credibility, as many outsiders know Nigeria is rich in oil. Stressing confidentiality is a gesture toward building some bond with the victim. Asking for your company

name, address and phone number yields information that might be useful in draining funds later on, but at the outset it is more likely that he is trying to gauge your level of interest.

A fifth example begins with a personal touch: he found the receiving address in a business directory. This is one of the more complex and sophisticated letters. It admits corruption and deception on the part of his famous "father," Sani Abacha, the late military ruler of Nigeria. It suggests a double deception: the owners of the vault-depository for the skimmed funds think the loot is jewelry, not cash. It invokes honor among thieves, as the writer suggests he is under oath not to reveal the secret workings of a diplomatic courier service. It openly suggests travel to Europe -- right away, since storage charges are mounting – and it requires a power of attorney and a future investment of other funds in the USA. Finally, in suggesting secrecy, it also hints at the issue of safety, perhaps a slight dash of danger to go with the frisson of illegality that the writer is betting will attract the recipient.

A sixth and final example makes use of the Sierra Leone civil war. This traces familiar ground; it seems plausible, invokes a religious blessing and asks for no confidential information at the outset. Indeed it trades on the vanity of the recipient, requesting help in locating a conservative (!) investment in the U.S.

We pursued five offers: setting up a separate e-mail account under as assumed name, pursuing questions and requests as far as we could, without actually giving up personal private information or traveling to Africa.[4] The object was to learn as much as we could about the process of the scam, short of a material commitment, risking life and treasure. To our first responses we received three quick and eager replies. They requested we make a phone call, to either the solicitor him/herself or that of a third party, either a lawyer or a security company, where the money resided. A vague second probe from our end elicited diverse replies. One provided more details, such as proof of deposit in the fake security company and later a photo of what he claimed to be himself and his now deceased father. (They were both obviously African, and one looked rather fierce.) A second refused to give us any concrete information until we offered more from our end. Replies came within a day or two, as they tried to accelerate the process. When our responses were slow they complained and questioned this -- one obviously getting angry. Our refusal to make a commitment (to send specific personal information or agree to fly to Nigeria or elsewhere), led to their loss of interest after several further exchanges.

In the literature one can piece together what happens when matters progress beyond conversation via e-mail. Brian Wizard, an American free-lance journalist and novelist, not only replied to several e-mails, he spoke to scammers on the

telephone and actually traveled to London and Amsterdam, where he met with a number of Africans. Wizard (2000) sent $750 as start-up funds, but he refused to advance the thousands requested. In 2004, a newspaper writer chronicled the exploits of "an ad hoc militia of counterscammers on several continents" (Schiesel 2004, G1,G7). These online vigilantes pursue a strategy of extended engagement, utilizing the same tactics as the scammers, sometimes receiving enough information to pass on to law enforcement and gain arrests.

Getting to the advance fee segment of the scam in a serious way seems to involve moving to phone conversations. Although revealing a bank name or account number is certainly a risk, experienced scammers realize that the big money does not come from the first part of the exchange. Sending such information indicates that the individual is a willing "mark." Banking security is now tighter than several years ago and outsiders cannot easily get to your money with simply a name, account number, and bank name (Marr 2003). The greater risk is that your bank account information permits application for credit cards, forging checks, or engaging in "crossfires" -- cashing forged checks and then withdrawing the money before the banks discover the fakes (Revill 2002). Solicitation of advance fees surfaces strongly when the mark begins to feel he/she is close to the money, having learned of details of how to extract it from a bank, a government account or a depository in Amsterdam, London, Liechtenstein, or in an

African country (Hill 2003, 25). The next stage reveals information that the money, if it is actual currency, has been altered to spirit it out of the country or has identifying marks upon it (McKinlay and Bell 2002, 1). Everyone in on the plot now knows this is an illegal operation. Scammers count on the sense of illegality exciting the mark; paradoxically, it now makes more sense than the claim that liberating this money serves a good cause and can be done smoothly, as the scammers disingenuously suggested at first. More important, it deters the mark from going to the authorities in the early stage.

Some victims are strung along for months and spend thousands of dollars, unwilling to believe they have been taken. A scam requires smart miscreants, but it is also needs believers. "It's like being a gambler, who throws good money after bad — the deeper you get in the more reluctance you have to back out," says James Caldwell, a supervisor in the financial crimes division of the U.S. Secret Service. "It's not unusual that we have seen victims lose more than $1 million." A U.S. Department of Commerce official elaborated, "Once people get hooked, my experience is they become more and more resistant to accepting that it's a scam, because they become vested in the deal. It's almost like … denial, they don't want to believe that it's not true." Many times a family member or friend of a victim will ask authorities for help. When officials receive the information, they try to talk the person out of becoming victimized. "We've done that quite a bit, where we've

talked people off a ledge, so to speak, and got them to come around and believe they're victims," Caldwell says (Ruppe, 2000; see also Robson 2002, 6).

> We've gone so far in the past to actually pull people off airplanes… We've gotten to these people and pulled them out of potentially either harmful or certainly cash sensitive situations and gotten them out. We're really quite proud of that…Clearly some people never ever come to the realization that they've been a victim to a fraud, and think that one more payment and their windfall is going to happen (Ruppe 2000).

Victims in denial then receive demands for about $10,000 to buy expensive chemicals needed to remove the identifying marks, to "clean the currency." Another excuse for an advance fee is the necessity for a lawyer to do the proper paperwork to transfer the funds. Sometimes the scammer offers to incorporate a fake company on behalf of the foreigner, as a conduit for the money (Murnaghan 2002). Another ploy requires a bribe for an official, who is holding up the process. Forwarding one fee usually yields a second, adding to already sunken funds, merely increasing the "deposit" on a giant windfall.

A late segment of the scam, and the most dangerous, is the request for the mark to travel abroad to meet in person, to insure the confidence of the people releasing the money. Our own experiment resulted in such a request within two weeks. Usually, an intermediary, a "disinterested" third party in a European

country is suggested, one in which a foreigner might feel more comfortable than in Africa. The Netherlands (multi-ethnic, officially tolerant, and an international *entrepot*) has served as this nominated country in several published accounts. There the mark would meet with well-tailored individuals with fancy cars at a five star hotel or in some official looking venue. More money is required, for one reason or another, but the big money is right down the street in the depository company. Again already sunken costs dictate one more donation. If this does not work, the scam can take a dark turn.

The final stage of the scam involves intimidation. Threats to detain the mark unless another, larger sum of money is forthcoming have been reported. Several foreigners have disappeared over several years while participating in these scams (Lin-Fisher 2002). In 1995 an American was murdered in Lagos; an American was ransomed in Johannesburg and another in Lagos, both in 2002 (Associated Press 2002, Roberts 2002); a Briton was tortured and beaten by his "partners" in Nigeria in 2003 (Brady 2003, 13). Wizard reports a particularly grisly denouement in Lagos. One victim was dismembered, despite a paid ransom, and then set ablaze (Wizard 2000, 158).

One of our own correspondents invited us to Nigeria rather soon in the relationship. Reports on such Nigerian travel adventures indicate that scammers offer assurances that everything is taken care of; you do not even need a passport

or visa to enter the country, they claim. Incredibly, people have accepted these terms; on arrival, the mark is informed it is a crime to enter the country without a passport. The victim is threatened with exposure unless a large bribe is forthcoming, c. $50,000 (Marr 2003).

A growing by-product of 419 scams is bank fraud. This takes exceptional technical know-how, co-ordination of a large number of people, and infiltration of the banking system. 419 scammers, who operate within a sophisticated network of criminal connections worldwide, are well-positioned to branch out. Reporters and police informants believe that a Nigerian crime syndicate exists today, which co-ordinates drug smuggling, arms traffic, money laundering, bank fraud and 419 scams. Information about bank names, addresses and accounts are traded. Concurrently, crime cells are increasingly recruiting individuals to infiltrate bank workers or bribe employees. Tony Thomas, Chief Inspector of the City of London Police, stated, "We are seeing an increasing [number] of people who are getting into banks and feeding details to outsiders. It is probably the most significant trend at the moment" (Catan and Peel 2003, 21).

South African banks were urged by their government to exercise caution when appointing new staff members, especially temporaries (Joffe 2003). Information on fat new accounts is transmitted and counterfeit money orders are instigated, yielding in today's parlance, "an E-bay scam." This works as follows:

someone is selling something on E-bay for $10,000. A buyer overseas wants to purchase the item and contacts the seller. The buyer says he has a friend nearby who owes him $15,000 and he is going to pick up the merchandise. The friend arrives at the seller's house with a check for $15,000 and the seller says, "But it is only $10,000." The friend suggests that the seller write him a check for $5,000 and everyone will be happy. As one might suspect, the $15,000 check turns out to be counterfeit; the seller gave up $5,000 and lost $10,000 worth of merchandise in the bargain.[5]

In an interview in Washington, DC, Brian Marr, who follows these matters for the U.S. Secret Service, described working on another case, where the victim brought a check, received from a 419 correspondent, to her bank, but suspected something was wrong. Twice the bank told her the check was good. Over a week later, the bank discovered the check was counterfeit. Banks apparently are not automatically liable in these instances. Banks can claim that an inexperienced teller had no way of knowing the check was counterfeit. No law or insurance deals with a bank's liability in dealing with fraudulent checks, which sometimes can take them more than a week to identify when drawn on a foreign bank. 419 scammers know this. Losses due to fraud, such as 419s, are rolled into the same numbers as bad debt. Such losses are written off and can yield tax breaks in the USA. Currently, the UK is working on legislation to makes banks liable for not

identifying fraudulent checks in a timely fashion (Marr 2003; see also Catan and Peel 2003, 21).

419 scams are also preying on banks and individuals via internet insecurity. Recently 419 scammers have set up websites that resemble legitimate banking sites. A mark is directed to such a fake website, as well as mock law firm sites (Economist 2002, 73). You log in with a username, and you are asked for personal information: bank account numbers, social security number, name and address. Since the sites look authentic, people comply. The only mis-identifying characteristics of the best examples are unknown international telephone area codes. (Citibank, as it occasionally reminds its customers, remains a prime target, impersonated at site addresses that include Citibank.com.) The occasional internet user, often ripe for 419s, becomes easy prey.

Highly publicized was a case where someone put up a fake website resembling South Africa's central bank and used it to swindle a British businessman out of 130,000 Pounds. The South African government declared the incident a "national priority crime" (Catan and Peel, 2003, 21). Scammers have used intercepted or illegally obtained bank customer information to telephone clients, posing as bank security officials to "re-confirm" personal security matters, such as a PIN. In some cases actual bank premises have been used to perpetrate frauds. Scammers posing as bank officials have set up shop in bank lobbies. The

Citibank lobby in Aldwych, London, was used to defraud a German industrialist of 1 million Pounds. 419 scammers also get involved in installing fake fronts on ATM machines, which grab credit cards. An "out of order" sign on a legitimate ATM directs customers to the altered one. Apparently there is a market for discarded cash dispensers for this purpose (Catan and Peel 2003, 21). Perhaps the most audacious ploy consisted in establishing a fake South African embassy in Amsterdam, in which a Saudi victim lost $100,000 (Schiesel 2004, G7).

A Brief History of 419s

"Advance fee frauds" have been around, reputedly, since the 16th Century. During England's war with Spain it surfaced as "the Spanish Prisoner" scheme. (It has recurred regularly; most recently in a 1998 film of the same name, script by David Mamet.) In April 1914 a letter was reprinted in the *Nigerian Customs and Trade Journal* from Arthur Hardinge, British Ambassador to Spain, calling attention to "the Spanish Prisoner swindle … established in Madrid and other Spanish towns... Assisted by accomplices in England…" Added to the letter was the note, "It appears that perpetrators of this fraud are still endeavoring to victimize Residents of the British Colonies and it is considered advisable that the public in Nigeria should be warned to be upon their guard."[6]

In its original form, wealthy merchants would be contacted by a stranger, perhaps a prison chaplain, claiming to be part of an attempt to smuggle the

sequestered child of an imprisoned family member (who might be dying) out of a Spanish prison. The target would earn a share of the reward for freeing the child or the imprisoned parent in return for helping finance a rescue of one or the other. (Spanish prisons, historically, have been imagined as particularly brutal.) Pity for the child joins avarice in keeping the target interested. The first rescue attempt would fail, as would a second, even more elaborate effort. One sees where this is heading. A convincing story would draw the victim into traveling to meet intermediaries and into increasingly bigger payments. While the story to entice people has changed, the basic principles of the scam have not.

The 419 mail scams seem to have originated in Nigeria in the 1970s and early 1980s (Tive 2002, 47; Wizard 2000, 157). Today they emanate from other countries outside Africa, such as Singapore, Russia, China (Hong Kong) and several places in the Caribbean (Straits Times 2002, Oldenberg 2002, C12). They started as unsolicited letters and later faxes, asking for assistance in transferring frozen or hidden funds, always secretly or illegally obtained, out of a West African country. Despite many promises, no case has been recorded where a foreign "investor" ever profited a single dollar, although there are two reports of partial refunds.

Some people still retain the early 1980s letters from the Nigerian "central bank" or the Nigerian "national petroleum company" as souvenirs. In the 1990s

the Nigerian government took advertisements in major newspapers in the USA warning of fraud via requests on fake stationery. With the invention of fax machines, perpetrators were able to reach many more people at a much faster pace. Moreover, by using a relatively new technology, schemers could emphasize the need for speed in responding to new "opportunities." Faxes permitted reaching the most desirable targets, business folk. Faxes – in their early years – also seemed more official, as well as urgent.

The invention and spread of the internet and e-mail have transformed the effort into a globe-girdling blizzard of instantaneous importunings. The U.S. Secret Service received ten times the number of scam complaints in 2002 as in 2001(Marr 2003); the U.S. Federal Trade Commission said such offers have reached "epidemic proportions" (Catan and Peel 2003, 21).[7] In addition to communicating instantaneously, the internet allows connection to a new world-wide group: ordinary people, newly-drawn to computers and e-mail, inexperienced in the ways of international commerce, but sometimes eager to participate in it. E-mail, direct, seemingly personal and instantaneously answerable, can now reach thousands of people a day.

Scope of 419s

To ordinary folk, these typical e-mails represent "delete" fodder, on a par with the mailbox spam that peddles sex performance stimulants, cheap Rolex

watches, discount pharmaceuticals, dirty pictures, and a variety of mortgage re-financings. Although most recipients trash these items robotically, to law enforcement they represent the iceberg tips of illegal activity of global dimensions.

Up to now, only a relative handful of persons actually sending these e-mails has been identified, much less apprehended, although they steal millions of dollars annually from unsuspecting victims. The full scope of the problem they pose remains comparatively uninvestigated by law-enforcement authorities in North America, Europe and Africa, and by the mass media, the general public, and the Africanist academic community.[8] Since a handful of persons have been maimed or killed while co-operating, non-official field-work remains a distinct risk.

Estimates of money losses vary wildly: that Americans alone lost at least $100 million in 2000 -- roughly what the U.S. sent to Nigeria in foreign aid that year (Ruppe 2000); that Advance Fee Fraud grosses hundreds of millions of dollars annually (U.S. Secret Service Advance Fee Advisory 2002, 3); perhaps more than $100 million annually worldwide in 2004 (Rian Visser, Inspector South African Police in Schiesel 2004, G7); and that victims worldwide may have lost an incredible $8 billion in one year (2001) via such fraud and theft ("E-mail Scam" 2002). According to the U.S. Secret Service, in the U.S.A. alone losses have hit at least a million dollars annually for several years (Catan and Peel 2003, 21). In Britain, the National Criminal Intelligence Service revealed that in 2002, 150

Britons lost 8.4 million Pounds to 419 scams (Brady 2003, 13). One reporter calculated that the "average victim" worldwide loses $342,000 (Lazarus 2003, G1), whereas counterscammers say that most victims lose about $3000 (Schiesel 2004, G7). Aside from concern for losses to legitimate economic activity in Africa and elsewhere, and sympathy for victims, these scams have elicited attention to a growing connection between the ill-gotten gains and more deadly illegal, international activity, such as arms and drug smuggling (Irish and Quobosheane, 84-93). Even more troubling is the allegation that these scams are not only tolerated but promoted by elements in the Nigerian government, since it is the third to fifth largest industry in the country – "the elites from which successive Governments of Nigeria have been drawn ARE the Scammers…"(Nigeria 419 Coalition website 2002, 1; see also Africa News 2003).

Identifying 419 Scammers

The craft of executing the contact in a 419 is said to be passed on in small groups and taught on a one-to-one basis (Marr 2003). The profit potential make 419 cohorts targets for organized crime. Amateur small groups may try their luck -- this is a business with easy entry and exit -- but the biggest, most sophisticated, and most profitable 419 scams are run by what the U.S. Justice Department dubs "the Nigerian Crime Enterprises." These are loosely organized syndicates, supposedly connected by "tribal" (Nigerians say this is code for Igbo) ties. But

law enforcement authorities note these alliances are not firm and groups materialize where profits are attractive. While the term "Mafia-like" has been applied, a hierarchy or structure remains unrevealed, making investigation extremely difficult, although U.S. law enforcement imputes tentacles in a number of nefarious enterprises (Buchanan and Grant 2001, 39-48, see remarks in Schwartz 2003, C5).

4-1-9 is a common epithet in Nigeria today, when a person claims someone is cheating. Many ordinary people believe that deception and corruption are required to achieve wealth and influence. A historical and cultural connection has been attributed by observers to the admired trickster, the con man, sometimes called "the feyman," who is also able to draw upon magic and witchcraft (Smith 2001, 803-826).

Aside from ambivalence about rapid acquisition of wealth but acknowledged corruption, ordinary Nigerians may silently feel pride in taking so many Westerners "to the cleaners." Although from a poor country by global standards, Nigerians are world class at racketeering, as evidenced by so much attention (see French 2004, 26, 31). Nigeria has been the capital of 419 fraud, although clearly other nationals and other countries are now involved. Singling out Nigeria does not make it a peculiarly Nigerian crime, although the scam letters of thirty years ago were sufficiently numerous and effective for the Nigerian government to warn

foreigners through newspaper advertisements. Africa's largest country by population (116.9 million, median age 17.3 years), suddenly enriched by oil and gas exploitation, Nigeria experienced the rise of an energy boom elite in the 1970s. Decades of misrule, a distorted economy and rampant corruption wiped out the middle class and produced enormous disparities between the well-off and the rest (Apter 1999).

> The [Nigerian] government spends over 80% of the budget running its own incompetent and corrupt bureaucracy. When not asleep at their desks, civil servants openly and cheerfully ask visitors to their offices for cash. Higher up the ladder, government procurement officers inflate contracts for anything from paper clips to luxury cars. Mr. Obasanjo uses several presidential planes and moves around town in a convoy of over 50 cars (Economist 2003, 46).

Millions of educated, English-speaking but jobless youth cannot find decent jobs at home, and most cannot emigrate to South Africa or U.K. or North America. Amidst persistent and manifold economic ills (Nigeria's annual per capita income is $3,000; GDP per head $350; [Economist Pocket World in Figures 2004, 176-77, 238]), financial fraud flourishes. A corrupt and inefficient court system and a government lacking effective authority do not help. Advance fee fraud scams could not operate without political connections. According to an investigation

reported in *Money* magazine, 419 scams in Nigeria are the second largest industry after oil (quoting Leon Wynter, Rapporteur, International Conference on Advance Fee [419] Fraud 2002, Nigeria 419 Coalition website, 2003). Based on his "diplomatic sources in Nigeria," Wizard (2000, ii) claims that 419s are the third to fifth largest industry in Nigeria. The underground economy reportedly accounts for 77 per cent of GDP, one of the highest percentages of any country in the world (Statesman's Year Book 2003, 1228). Nigeria's rackets reflect the growth of "cowboy capitalism" – unruly entrepreneurialism flourishing within a lawless environment. Enforcement of rules merely competes with, and does not overcome, force and fraud.

Finally, there is Western complicity. One cannot rule out the demonstration effect of Westerners extracting millions of dollars from Nigeria and elsewhere in Africa via bribes and dominant partner arrangements. Nigeria, probably more than other African countries, provides numerous examples of big Western companies paying bribes to win contracts. To most Africans, international commerce means draining Africa of natural resources in unequal partnerships with foreign governments and multi-national corporations. It takes little imagination to believe that capitalist enterprise means a big hustle, where all gains are ill-gotten, and where the little guy gets ahead only by imitating the big guys.

Combatting 419s

Increasing wariness regarding Nigerian entrepreneurs caused the U.S. Department of Justice for a brief period in mid-2002 to secure a court order to open every piece of mail from Nigeria passing through JFK airport in New York. Almost 70 per cent of the mail involved scam offers (Weber 2002; see also Chen 1998, B1,7). Four Nigerians and two other African companions were arrested in Atlanta in 2002 for e-mail fraud and drug trafficking. Seized with them were drugs, computer equipment and false identification papers (Husted 2002). Two Canadians in 2002 were arrested for fronting for Nigerians in recruiting nearly fifty cohorts to defraud others via 419 scams (Perraux 2002, A4). Two "godfathers" of 419 frauds from Nigeria, F.C. Ibe and J.O. Onugoagu, were arrested in England in 2002 (Penman and Greenwood 2002, 26). The Royal Canadian Mounted Police announced the dismantlement of a Nigeria-based phone scam, using a Toronto "boiler room" that had claimed 300 victims in 2001 (Canada News Wire 2001). The U.S. Secret Service, since 1995, has worked with the U.S. Department of Commerce, and Nigerian and other foreign authorities, to counter such operations. In 1996 the U.S. Secret Service, in co-operation with the Nigerian Federal Investigation and Intelligence Bureau, arrested 43 persons in sixteen Nigerian locations, along with much evidence of fraudulent practices ("Operation 4-1-9," 1996). Stating that 17 persons were killed in Nigeria as a result of 419 scams, U.S. Congressman Edward Markey (Massachusetts) in 1998 introduced the Nigerian

Advance Fee Fraud Prevention Bill (Markey 1998). The bill did not pass, but it caused a brief flurry of discussion. In August 2000 the U. S. Secret Service opened an office in Lagos to share information, technical expertise and some resources to help Nigerian authorities battle advanced fee fraud and other Nigerian criminal activity, such as money laundering and counterfeiting.

Scammers today are moving into South Africa, evidenced by recent arrests there of several supposed kingpins of 419 fraud, A. Odonoko and his wife and 15 others carrying Nigerian passports (BBC Monitoring Africa 2002, Africa News 2003). An authoritative observer calls South Africa "Africa's capital of organized crime" (Ellis 1999, 50). Aside from the cosmopolitan attraction of South Africa, the largest and most dynamic economy on the continent, foreigners were growingingly wary of "Nigerian" e-mails. The economic and communications infrastructure in South Africa makes all sorts of business easier and cheaper. South Africa's borders remain porous, while its economy is a magnet for illegal immigrants from elsewhere in Africa. Recently, observers have seen South Africa replacing Nigeria as "the 419 capital of the world"(Africa News 2003a, see also Economist 2004a). A comprehensive report observes that advance fee fraud scams, operating out of South Africa, now take many forms: transfer of funds linked to over-invoiced contracts; contract fraud; conversion of currency – "black dollars" (the old money-washing scheme); the sale of diamonds and other precious items at

below market value; fraudulent purchase of real estate; fraudulent disbursement of money from estates; extortion; and clearinghouse scams (Irish and Quobosheane, 86-87). Yet the move to South Africa is double-edged. The South African government and its police are better equipped to combat 419 fraud, which, ironically, further disperses 419 gangs to almost anywhere there is an internet café.

Any government's effort to combat 419 fraud is contingent upon foreign official partners also addressing the problem. Over the years pressure on the Nigerian government has produced some results. With the Advance Fee Fraud and Other Related Offences Decree of 1993 (African News Service 2001), General Sani Abacha, Nigeria's then military ruler, appointed a ministerial task force to combat drugs and fraud networks, which he believed to be connected. By 1995 Nigerian authorities claimed investigation and arrest of 1,200 suspects, but apparently convicted none. Most visible of the arrests was Fred Ajudua, who aspired to be the black Robin Hood. The frauds, he alleged, were compensation from white men for slavery and colonialism (Economist 1995, 36, Africa News Service 2003). Nigeria's current president, Olasegun Obasanjo, inaugurated in 1999, identified 419s as "one of the priority issues for resolution, having been noted as one of the principal causes of loss of life, property and investment" (Africa News Service 2001, 2001b). Nigerian officials talk a good deal about combating 419 fraud. A deputy governor of the Central Bank of Nigeria [CBN],

Dr. Samsudeen Usman, said at a conference on 419 fraud in New York in September 2002 that the apex bank [CBN] has intensified enforcement of relevant laws requiring banks to prevent the use of their facility to perpetrate 419 or the laundering of money. If a bank was found to have been careless in allowing a criminal to defraud another person, it would be made to refund the money involved. He said the Central Bank had already caused a commercial bank to refund $400,000 to a defrauded American (Report of the International Conference on Advance Fee [419] Fraud, 2002, see also Africa News Service 2000). CBN has established a task force on economic crime and extended its surveillance of 419 activities to other financial institutions such as money exchanges, mortgage institutions and others. The conference on economic crimes, organized first in 2000 by CBN, is supposed to occur annually.

Yet performance in combating 419 fraud remains flaccid; in August 2001 the Financial Action Task Force of the International Monetary Fund listed Nigeria as a non-co-operating country (African News Service 2001a). African governments, aside from lacking resources, do not view 419 scams as a priority crime; it is like targeting pick-pocketing as a serious pursuit. Some people –not only Africans -- believe that if some Westerners are dumb enough to fall for the scam, it is their own fault.

Nevertheless arrests continue. South Africa has tasked their elite police unit, "the Scorpions," to seek 419 networks. In 2003, after a 20 month investigation, the Scorpions netted a titan of 419 fraud, Phil Okafor, legal advisor to the South African branch of Nigeria's ruling People's Democratic Party. In addition to the high profile arrest of Okafor, South Africa has placed 3,000 Nigerians in detention, many in connection to 419 frauds (Africa News 2003). In March 2004, Rian Visser, inspector and electronic fraud investigator for the South African Police Service established an unofficial website, www.419legal.org, as a clearing house for for advance fee fraud information (Schiesel 2004, G7). The U. S. Secret Service, in conjunction with British National Criminal Intelligence Service and the Royal Canadian Mounted Police, have been working to aid the Scorpions in South Africa (BBC Worldwide Monitoring Africa 2002). All these parties co-operated in 2001 in the major bust of a Toronto area fraud ring that had claimed 300 victims, with individual losses ranging from $52,000 to over $5 million (Canada Newswire 2001). The U.S. Department of Justice has fashioned tools to investigate and prosecute 419s, including undercover operations, using targeted businesses, and the use of statutes dealing with mail, wire, fax and phone fraud.

Yet 419 fraudsters remain elusive. Police report that operations shut down and move quickly. Global internet connections with today's technology make the origin of e-mails extremely difficult to trace without a major mobilization of

investigatory resources.[9] Tracing an e-mail means working laboriously backwards-- a time consuming process that involves subpoening an internet server, such as Yahoo, and requiring much technical co-operation. E-mails can now bounce from one server to another, disguising their origin. Scammers who claim to be in Lagos or Abidjan could be sitting in an internet cafe in Hong Kong or Amsterdam. In addition, 419 scams remain an underreported crime. Victims are embarrassed about coming forward, but they also fear they might have done something illegal. Police cannot legally pursue individuals on the basis of e-mails alone. A non-threatening e-mail is deemed commerce or free speech. A monetary loss must occur. By the time a server might be found, the scammers have scrammed.

419 frauds themselves create more damage than personal financial losses. The prevalence of their advertisements in the popular experience, especially among Western professionals and business people, undermines legitimate African, and especially Nigerian, business (Haliechuk 1994). The effects of 419s are also damaging at the human relations level: for instance, during the World Cup competition almost a decade ago, many Nigerian soccer players wanted to move out of their training site in Texas because the local police had warned the community against accepting credit cards from the players (Shiner 1994). E-bay now has warnings on the website, not specifically targeting Africans, but apparently in response to the 419 scams.

So why do these scams persist and such offers continue to grow? The obvious answer is greed, suckerdom and low cost profits. It is estimated that the scammers need only a one per cent success rate to make a profit (Brady 2003, 13). One person, using whole lists, could send out anywhere from 1,000 to 100,000 scams a day. If 20,000 messages are sent out daily and one per cent responds, that is 200 people to work with. If ten people in one location are sending e-mails, that is possibly 2000 responses every day. If the average loss per victim, as some have previously estimated, tops $300,000 and one per cent of 200 people are conned, that could amount to potentially $600,000 a day. The internet is adding new users every day at an exponential the rate, 900 per cent in the one year 2000, according to Jonathan Rusch, U.S. Department of Justice (Report of the International Conference on Advance Fee Fraud 2002).

Should we worry about 419 fraud? There are two compelling reasons for serious concern. One: 419s may now be so embedded in the Nigerian economy and society that they are now a permanent poison drip. Anecdotal evidence now exists of "reverse 419s:" Nigerians in Europe preying on Nigerians at home, demanding money to clear certain goods supposedly waiting to be shipped out; and Nigerians in Europe and North America targeted by a "physician" at home, who seems to know the family's name, and who needs funds to aid a relative supposedly involved in an accident. A "criminalized state" in Nigeria, and the

expansion of criminal activity in South Africa – the two most influential states in black Africa – represents a gathering threat to legitimate commerce, as well as to social bonds over the whole continent. For most ordinary North Americans and Europeans on the internet, 419s are probably the only contact they have with Africa. Two: the money earned in 419 fraud may be being used to support other types of more violent and deadly crimes. Global crime enterprises, which include 419 operations, lead to connections to drug trafficking, arms dealing and assassinations.[10] Travelers and researchers in Nigeria report rumors that Igbo Nigerians dominate the retail trade in crack cocaine. An authoritative report confirms that "Nigerian networks are centrally involved in bringing significant amounts of cocaine into South Africa and many have direct links to the source countries in Latin America" (Irish and Quobosheane 2003, 88). U.K. and U.S. officials have thus far played down a possible terrorism connection, although they admit that Nigerian gangs are active in the heroin trade, which would bring them into business relations with clandestine elements in Afghanistan and Pakistan (Catan and Peel 2003, 21).

In December 2003 both legislative houses of the U.S. Congress passed conforming bills to reduce and regulate unsolicited e-mail, which President Bush later signed. By August 2004 U.S. federal officials arrested or charged a number of persons with crimes connected to junk e-mail, identity theft and other online

scamming. Neither international nor African e-mails were singled out (Hansell 2004, C1 ,6, also Andrews and Hansell 2003, A1, C 14, Lee 2003, C3, Tanaka 2003, C1,3). It remains unclear how the "spam busting" law in the U.S.A. will affect advance fee schemes and scammers, especially those located outside the country. So far the fraudsters have proved sufficiently resourceful to continue to find new ways to discover new victims.