

Nigeria - [419 Coalition](#) 2007 News on Nigerian Scam / 419 Operations

19 DEC 2007

From the Nigerian newspaper, The Punch:

Three Nigerians arrested at MMIA for duping Chinese lady

By David Amuwa and Oyetunji Abioye

Three Nigerians have been arrested by security men for allegedly duping a Chinese lady, Tseung C. Barbara, of 3,000 euros.

Jolly Akpoge, Michael Ogbile and Cyrus Ovie, were arrested on Sunday at the Murtala Muhammed International Airport, Ikeja, Lagos on Sunday when they went to receive Barbara, who arrived aboard China Southern Airline.

The trio, who motivated the Chinese to come to Nigeria with lots of money and materials, had deceived her that her French man friend, whom she had a rift with, was in the country.

On arriving at the MMIA on Sunday, Barbara was surprised to see a black man, Jolly, instead of her French man friend, whose name our correspondents could not ascertain.

At this point, she became furious and started lamenting. She created a scene that attracted the attention of security men, who intervened and arrested the trio and handed them over to the officials of the criminal department of the Airport Police Command at about 7pm.

Our correspondents learnt from a reliable source that the suspects had formed a syndicate to swindle the Chinese lady whom they had been communicating with through the Internet.

Barbara said she had a misunderstanding with her French friend and was looking forward to a reconciliation with him when suddenly, Akpoge started communicating with her, pretending to be the French man.

She added that she fell into the trap because Akpoge got all the necessary information to convince her beyond any doubt that he was the French man. The three Internet fraudsters were said to reside at Ajegunle.

Barbara claimed that Akpoge might probably have got information about her from one Ovie whom she said had once lived in Beijing.

Our correspondents learnt that Barbara had sent 1,000 euros and 2,000 euros to Akpoge at different times.

The officials at the criminal section of the command who spoke to our correspondents on the case, confirmed the fraud.

Our correspondents sighted Barbara at the command but one of the officers did not allow an interview with her.

Two senior officers of the department, however, said the suspects had confessed receiving the first batch of the money but denied the second.

19 DEC 2007

Sent in by a concerned Nigerian, article from the Nigerian newspaper Vanguard:

Ade Bendel sentenced to six years Imprisonment

Written by Kayode Matthew

An Ikeja High Court yesterday sentenced a Lagos based businessman, Mr Adedeji Alumile a.k.a. Ade Bendel to six years imprisonment for obtaining the sum of \$600,000.00 under false pretence from an Egyptian general in 2003. Justice Muniru Olokoba who handed down the verdict while delivering judgement in a one count charge preferred against the accused person also ordered Ade Bendel to refund the money to the Egyptian. According to the charge preferred against him by the Economic and Financial Crimes Commission, Ade Bendel claimed to be the owner of a company called Worldwide and went to the office of the Egyptian national alongside one Olafemi Ayeni in 2003 to deceive him into parting with \$600,000.00 to enable them buy chemicals that could be used to clean some paper notes. They also claimed that the chemicals could remove security covers from the notes.

It however turned out that the company called Worldwide never existed and no chemicals were bought. The Egyptian then lodged a complaint with the anti-graft agency which led to the arrest and detention of the accused since May 2003. On his arraignment Ade Bendel pleaded not guilty to the charge but later amended his plea and pleaded guilty when he struck an agreement with the EFCC to refund the money to the Egyptian.

After the judge had found him guilty of the offence, the defence counsel then pleaded with the trial judge to temper justice with mercy. According to him, the accused is a first offender, he is a young man of 41 years with a wife and children. The accused has made full restitution and paid the sum of \$200,000.00 to the complainant which has been deposited with the EFCC. It is important that the accused be given full rehabilitation as the maximum sentence for the offence is seven years.

In his judgement, Justice Muniru Olokoba said "the offence is an international embarrassment to the nation and the court does not have mercy with such offence. To serve as deterrent to the present generation and the upcoming generation not giving the accused a full weight of the law is inappropriate. I hereby sentence the accused to six years imprisonment on the one count charge."

Here the the URL of the article for as long as it is good:
http://www.vanguardngr.com/index.php?option=com_content&task=view&id=3263&Itemid=43

Several Nigerian newspapers, including ThisDay, The Punch and others also covered the story, here is the URL of the ThisDay piece for as long as it is good:
<http://www.thisdayonline.com/nview.php?id=98390>

4 DEC 2007

From the Nigerian newspaper The Daily Independent:

10 Nigerians, Others Arrested Over \$2.1b Fraud In Canada

By Wisdom Patrick, Snr Correspondent, Lagos (with agency report)

Detectives in five countries, including Nigeria, have arrested no fewer than 77 people - among them 10 Nigerians - and seized about \$2.1 billion in counterfeit cheques bound for the United States in a sweeping crackdown that included arrests in Canada and Nigeria.

The investigation, which lasted eight months, targeted scammers in The Netherlands, Nigeria, and England who specialised in defrauding people by sending them fake cheques and asking for a portion of the money back.

Henry Oshingbene, 39, of Brampton, was charged with four counts over a \$5,000 fraud for allegedly contacting residents in the U.S. and telling them they had won one million euros in a lottery but needed to pay fees to get the money.

The two victims allegedly lost more than \$290,000.

Stephen Foster, Director of the Canadian Fraud and Commercial Crime branch of the Canadian police, said officials across the country had seized nearly 5,000 counterfeit financial documents since April with a face value of more than \$13 million.

The mass distribution of phoney cheques, money orders and the likes is a growing concern in Canada, Foster told a news conference hosted by the U.S. Postal Inspection Service, with Economic and Financial Crimes Commission (EFCC) Chairman, Nuhu Ribadu, in attendance.

It is a borderless crime that has enormous financial implications for citizens, governments and the economy, he said, adding: "I don't think Canadians should worry any more or any less than the Americans and the Africans. We have similar financial systems. The pitches are similar. They're just as plausible."

It is easy to fall prey to the schemes, he said, because they sound so reasonable and much of it is done by e-mail.

A new tenant, for instance, may send a cheque for the deposit and rent, but then ask for some cash back to cover unexpected expenses. Meantime, the cheque that goes into the landlord's account bounces because it was faked. If the money was withdrawn, it must be paid back to the bank.

There are a lot of other scams, including buying an item in an online auction and paying more than the purchase price so some of the money can be forwarded to someone else to cover the shipping costs.

"I could see someone falling for that kind of pitch," said Foster. "If you don't know who you're dealing with, then maybe you shouldn't take that money." People who do fall for the scams lose an average of \$3,000 to \$4,000 each.

"There is no room in the mail for any of these phoney come-ons," added U.S. Postmaster General, John Potter.

Retired people have lost their nest eggs and young families have been defrauded of their savings for a home, Potter said. Many of the cases originate in The Netherlands, where West African con artists operate from Internet cafes, stated Johan Van Hartskamp, Commissioner of the Amsterdam Police.

"I suspect these scams have been around as long as there's been money," Laurel Kamen, Vice President of Consumer Affairs for American Express said. "What's new today is the Internet."

According to Susan Grant, Vice President of the National Consumers League, complaints from Americans about phoney cheques have increased by 60 percent in 2007.

The scams hit people of all ages and education levels.

For instance, in Nigeria, a Minister in the administration of former President Olusegun Obasanjo was a victim, when he allegedly wanted to buy a house in Canada and was swindled by fraudsters to the sum of \$150,000.

The Minister had to forfeit both the house and the money, because in Canadian law, both the fraud victim and suspect have some price to pay.

The criminals have come up with a new twist to the scams. In the past, many people who responded to 419 e-mails simply did not have the money to send the scammers for the fees and other charges needed for the victim to get their millions.

To get around that problem, and keep a willing victim in the scam, the fraudsters have developed financiers who will give the victim a loan until they receive that trunk box of money or their lottery winnings.

This financier is just another of the gang member playing a role in the scam. He always grants the victim the loan, and often they offer the victim their choice of two options to receive the money from the financier.

They will send the victim a cheque for the amount of the loan. The victim is to deposit the cheque in their bank account and then draw out the amount of the fees and charges and wire them to the scammer via Western Union.

The only problem is that the cheque is counterfeit; and it is not usually caught until it reaches the issuing bank, long after the victim has wired the money to the scammers.

Here is the URL of the article for as long as it is good:
<http://www.independentngonline.com/?c=117&a=6624>

12 NOV 2007

From the Newark New Jersey Star-Ledger:

Web scam artists get taken in, too

BY J. SCOTT ORR
Star-Ledger Staff

Just who is Babatope and why is he eating a loaf of bread while holding a dead fish on his head?

To prove, of course, that despite his plea for money and despite his location in the Internet swindle epicenter of Nigeria, he is one honest and God-fearing man.

Babatope is an Internet scammer, the kind responsible for those ubiquitous e-mails offering untold wealth to anyone willing to help move their funds to the U.S. It might be a \$20-million estate entangled in government regulation, or a \$30-million charity fund that needs an American handler. The scammers' stories are limitless and ever-changing.

But in this particular case, it was Babatope who was the target of a scam that cost him months of effort and the humiliation of posing for a goofy picture to prove his devotion to the fictitious Church of Fish and Bread.

Babatope is one of the countless victims of so-called scambaiters, a decentralized group of savvy netsters who spend their time turning the tables on Internet scam-artists by luring them into believing they are a bunch of wealthy patsies.

The scambaiter's goal: to waste the scammers' time and sap resources that would otherwise be used to try to bilk more vulnerable targets. When possible, making the scammers look foolish is a bonus.

If you've got an e-mail account, you have no doubt encountered scammers like Babatope, whose swindles are called 419 scams after the section of the Nigerian criminal code that outlaws Internet scamming.

A typical 419 scam e-mail will seek your help in liberating a sum of money, often tens of millions of dollars, in which you will share once the deal is complete. After the scammer establishes a relationship with you, he or she then requests money, often to offset "transfer fees," bribe officials, or otherwise eliminate some snag that stands between you and a million-dollar pay day.

Of course, there is no \$20 million sitting in some foreign bank account and no ton of gold bullion uncovered in an Iraqi battlefield. Send in the \$1,500 to overcome that last bureaucratic hurdle and chances are you won't hear from the scammer again unless it is a request for just a bit more money.

The FBI's Internet Crime Complaint Center received 207,492 complaints during 2006, accounting for losses of nearly \$200 million, with median losses of \$724 per complaint. But according to the center's report for 2006, the median loss for 419 scams was \$5,100.

For scambaiters, like Shiver Metimbers -- the screen name used by the scambaiter who conducted the elaborate counter-scam that frustrated Babatope -- every online come-on is an opportunity for some fun.

"They have the ability to swindle the swindler. ... What they're actually doing is sapping the energy the 419 scammer would be focusing on someone else," said Robert Siciliano, who heads the Boston-based IDTheftSecurity.com, which helps protect Internet users from scams

Shiver Metimbers, the scambaiter who played Babatope, is in reality Michael Berry, or at least that's the name the Englishman used as the author of "Greetings in Jesus Name! The Scambaiter Letters," published last year. The book details dozens of scambaiting triumphs, including convincing scammers to send humiliating photos of themselves, to submit various artworks, even to send him money.

"If they believe that holding a silly sign or posing with a fish on their head is going to get them some easy money from a gullible victim, then they will do what it takes," Berry writes on his Web site, 419eater.com.

Sites like 419eater.com, scamorama.com, thescambaiter.com, scambusters.org and others display logs of their communications with scammers along with "trophy" pictures and videos of scammed scammers. While they encourage scambaiting, they also warn that those who engage in the "sport" should remember they are dealing with criminals and that getting too close could be dangerous.

C.A. Pascale, the coordinator of the 419 Coalition, which strives to educate Internet users about scams, said in an e-mail his group applauds the work of scambaiters, but worries "that at some point a baiter may make an error and be harmed by a 419er, though this has not happened as yet to our knowledge."

"While we appreciate and often privately applaud the work of the scambaiters, we do not publicly advocate it," he said.

Frances Zollers, a professor at the Whitman School of Management at Syracuse University who has studied Internet fraud, said scambaiters have little chance of making a significant impact on a crime that has grown exponentially in recent years.

"If I'm a scammer and I start getting this kind of noise from a target, I move on. The very bad news is that the scambaiters are probably going to go away before the scammers who will resume preying on a more vulnerable population," she said.

As for the scams themselves, experts urge caution and common sense. As the Nigerian Economic and Financial Crimes Commission, which tries to police the crime, notes on its Web page: "Please be aware. You have been warned."

J. Scott Orr may be reached at sorr@starledger.com.

Here is the URL of the article for as long as it is good:
<http://www.nj.com/starledger/stories/index.ssf?/base/news-12/1194846074199800.xml&coll=1>

11 NOV 2007

There is an interesting piece concerning phishing and 419 via Facebook and free email account providers etc. in today's New York Times BITS (Business, Information, Technology and Society) section along with responses from the readers. It is too long to put up here, but here is the URL for as long as it is good:

<http://bits.blogs.nytimes.com/2007/11/09/e-mail-scammers-ask-your-friends-for-money/?ex=1195448400&en=50a0f8a96645c72b&ei=5070&emc=eta1>

3 NOV 2007

From the Nigerian newspaper The Punch:

Forgery: 25-year-old undergraduate jailed 34 years

By Tony Amokeodo

A 25-year-old undergraduate, Mr. Omoniyi Sanlola, was on Friday sentenced to 34 years imprisonment by a Federal High Court in Lagos for fraudulent activities and forgery.

Sanlola was arraigned before Justice Tijani Abubakar by the Economic and Financial Crimes Commission on a 34-count charge of fraudulently and knowingly forging United States Postal Services money order payable to various people on November 15, 2006. The offence is punishable under Section 1 (2) (a) of the Miscellaneous Offences Act No 20, 1984 as amended by Act 62 of 1999.

Sanlola, a final year student of Geology at the Ogun State University, Ago-Iwoye, had pleaded guilty to the 34-count charge that was read to him before the court. Though the convict was arraigned by the EFCC, he was arrested by the operatives of the National Drug Law Enforcement Agency at the Ogun State border on his way to the Republic of Benin.

He was said to have been in possession of seven sealed envelopes containing 34 forged postal order cheques when he was arrested by the NDLEA. Though he was sentenced to 34 years in prison on each of the 34 counts, the convict is expected to spend one year behind bars, as the prison terms will run concurrently.

In his judgment over the matter, the judge said the crime had dented the image of Nigerians who were into legitimate business abroad.

Here is a link to the article for as long as it is good:
<http://www.punchontheweb.com/Articl.aspxtheartic=Art2007110315372173>

2 NOV 2007

From the Canadian News Wire:

OPP Bust Counterfeit Cheque Ring

TORONTO, Nov. 2 /CNW/ - Officers from the Ontario Provincial Police Anti-Rackets Section arrested three persons in connection with the production and mass mailing of counterfeit cheques throughout North America.

This investigation was primarily focused on the "lab" where the fraudulent cheques were manufactured. The scheme was accomplished by preparing counterfeit cheques and their supporting documentation in regards to charities, lotteries, personal loans, etc. In most cases the accused attempted to legitimize their fraudulent schemes by using publicly available, real charity and lottery identifiers.

This was a partnership investigation involving: Vancouver Police, United States Postal Inspection Service, Canada Post Corporation, York Regional Police, Peel Regional Police, all Major Financial Institutions within Canada, and the Ontario Provincial Police, Anti-Rackets Section, Identity Crimes and Forgery Investigation Unit as the lead agency.

Financial investigators and police scrutinized numerous complaints throughout North America. Over 55,000 individual complaints, representing a face value of over 400 Million Dollars in potential loss.

Between early 2005 and November 2007 a total of 55,000 complaints were registered with Phonebusters, The Canadian Anti-Fraud Call Centre. Of those 55,000, 974 originated from within Ontario bearing a total actual loss of 1.3 millions dollars.

Police executed five search warrants and seized several computer systems, printers, scanners, counterfeit US currency, and thousands of cheques in various stages of production.

Charged are:

Godwin Friday ANIGOZIE, age 39 of Woodbridge, Ontario, one count of fraud over five thousand dollars, utter forged document, and conspiracy to commit fraud.

Joanna FERENSOWICZ, age 22 of Woodbridge, Ontario, one count of fraud over five thousand dollars, utter forged document, and conspiracy to commit fraud.

Tamara CARTER, age 33, of Brampton, Ontario, one count of fraud over five thousand dollars, utter forged document, and conspiracy to commit fraud.

All three are scheduled to appear in Old City Hall Court, Toronto, on December 17th, 2007.

The investigation is continuing.

For further information: D/S/Sgt Andy Mayo, OPP Anti-Rackets Section, Identity Crimes and Forgery, Investigation Unit, Phone: (705) 795-0985

Here is the URL of the article for as long as it is good:
<http://www.newswire.ca/en/releases/archive/November2007/02/c3704.html>

21 OCT 2007

From the Los Angeles Times:

Fake-check schemes grow in sophistication

An international crackdown has had limited success as scammers, many operating out of Nigeria, discover new ways to play an old game.

By David Colker, Los Angeles Times Staff Writer

It was Fred Tracomm's lucky day. Two checks came in the mail to a Chicago office -- one for \$4,000 and the other for \$4,000.50. Both were made out to Fred.

But Tracomm wasn't expecting any checks. In fact, he doesn't exist.

The checks were part of a fake-check scheme, a rapidly growing scam that federal authorities believe mostly originates in ground zero for so much of the fraud plaguing the Internet: Nigeria. The U.S. Postal Inspection Service announced this month that it had seized \$2.1 billion worth of the fake checks this year through joint operations in Nigeria and other countries.

The Postal Inspection Service also established a website, with the financial support of several banking institutions, to educate the public about the scams. It's at www.fakechecks.org.

The feds had an easy time seizing Fred's checks. That's because the scammer had inadvertently sent them directly to the Midwest office of the Federal Trade Commission, which for years has been getting advertising mailers addressed to Fed Tracomm.

"We get junk mail like everyone else," said Steven Baker, director of the FTC office. "So, we're on mailing lists that get passed around and sold. Somewhere along the way, someone added an 'r' to the name."

Thus was born Fred, who was instructed in a letter accompanying the checks to deposit them and then notify the sender by e-mail. Fred was to wire a portion of the money back to the sender and keep the rest.

The checks were counterfeits but looked disturbingly real.

"You can buy check stock at any big office supply store," said Renee Focht, an inspector with the Postal Inspection Service's Los Angeles division, headquartered in Pasadena. "They use sophisticated printers to print the checks, and sometimes even embed security features in them, making them seem more legitimate."

Banks usually make funds available from a company or certified check before the check actually clears.

"People think that when funds are available, it means the check is good," Focht said. But later, when the check bounces, the bank wants the money back. All of it, not just the portion the victim was told to keep.

These fake-check scams mark a shift away from the traditional advance-fee Nigerian scams in which a potential victim would be contacted and told that he or she was owed a huge amount of money. Or perhaps the dictator of a country had died and a silent partner was needed to get his secret fortune out of the country. The most imaginative version lures victims with online ads featuring pictures of cute puppies that somehow got stuck in West Africa and are in need of good homes.

The intended scam victim would be asked to pay a fee to cover expenses, and the money would start rolling in or the puppy would be delivered to their loving arms. Except that would never happen.

The advance fee scams are still around, but they seem almost quaint.

"The dead dictator is dead," Baker said.

Fake-check scams, which took up the baton, have a distinct advantage.

"People get a check -- a physical piece of paper -- in their hands, so it seems more real," Focht said. They are told to wire a substantial portion back to cover taxes, customs fees or other matters.

Usually, the scheme is more detailed than the simple note addressed to Fred. Potential victims are told that they won a sweepstakes somewhere in the world or are perhaps getting a grant to be used to further their education.

One of the more common schemes involves foreign companies looking for people willing to deposit funds for them in U.S. accounts.

A recent example, provided by the Postal Inspection Service, involved e-mails supposedly sent from Teikoku Oil & Gas Co. in Tokyo. The firm needed "representatives" who could handle funds to be paid out to U.S. or Canadian customers.

Teikoku does exist. It has put a notice on its website saying it has nothing to do with the e-mails and that they are false.

Another widespread variation on the scam is from the supposed owner of Susan Art World in London. The e-mails -- and in some cases ads placed on Craigslist and other online venues -- go into detail about the wonderful life Susan has with her husband, children and cats. And she just loves to paint, obligingly including images of her creations. But "customers in America always offer to pay me with U.S. postal money orders" that she has a hard time cashing.

In exchange for cashing the postal orders, she offers a 15% commission.

If the nature of the offer wasn't enough to identify this as a fake-check scheme, there is also the fact that in various copies of the e-mails, the name of the husband and the number of cats varies. Not to mention that the paintings of children, geishas and landscapes would have a tough time passing muster at a sidewalk sale.

The seizing of fake checks in the Postal Inspection Service joint operation was mostly done in Nigeria by that country's law enforcement agencies. "The government of Nigeria recognizes that it has what could politely be called an image problem," said Douglas Bem, a postal inspector in Washington.

Bem said the joint operation had developed ways of identifying suspicious envelopes. He declined to say what they were looking for. But there were little or no restrictions in opening the envelopes in Nigeria.

"Here in the U.S.," Bem said, "we would need a court order."

The eight-month international operation resulted in 60 arrests in the Netherlands and 16 in Nigeria -- small numbers, considering the scope of the problem.

"We are not deluding ourselves into thinking we have stopped the flow of fake checks into this country," Bem said. "The investigations in Nigeria by the Economic and Financial Crimes Commission are continuing."

The name of that agency might sound familiar.

An e-mail from the EFCC hyping its investigative efforts is popping up all over the Web.

The message says that \$322 million of ill-gotten gains had been recovered.

Then, in the middle of the e-mail, comes this: "Your name was given to us by one of the fraudsters in our jail house, that he collected money from by tricks.

"Our action now is to refund back money to foreigners who lost money to these thieves [sic]. We are paying back from the money we recovered."

It's yet another scam. Chances are, Fred got the same e-mail.

david.colker@latimes.com

Here is the URL of the article for as long as it is good:
<http://www.latimes.com/business/la-fi-consumer21oct21,0,1195949,full.story?coll=la-home-center>

4 OCT 2007

From the Mirror.co.uk, which is the online version of the UK Daily Mirror we believe:

Multi-billion fraud gangs are nailed

by Penman & Sommerlad

Scambusters across three continents have dealt a hammer blow to Nigeria's No.1 cottage industry - fraud.

Thousands of bogus ID papers and bank documents have been intercepted along with 15,000 fake cheques en route to potential victims in Europe and America.

They could have been used to con tens of millions of pounds through a range of "advance fee" and "cheque overpayment" scams.

Examples of advance fee frauds include bogus lotteries and "I'm the son of a late African dictator with millions in the bank" spam.

Victims are persuaded to hand over large sums of cash in the hope of earning back much more.

The closely-linked cheque overpayment fraud adds a twist where the victim thinks they've already been paid but ends up out of pocket when a cheque bounces.

One victim, Harpreet Smith, advertised her car on a website.

Mario Grima from Malta offered to buy the £650 motor and have it shipped. He sent a cheque for £3,000 and asked Harpreet to forward the difference, less fees, to a shipping firm in Benin, West Africa.

She banked the cheque and waited for it to clear before sending £2,245 by Western Union to "shipper" Tomas Frank.

One week later she plunged £3,000 into the red as the cheque bounced.

"I am already in debt," said Harpreet of Rotherham, S. Yorks. "I am a single mother of three and I've been off work with stress for weeks because of this."

This 419 fraud - named after the relevant section of Nigeria's penal code - is thought to cost the UK over £1 billion a year.

Serious Organised Crime Agency detectives flew to Lagos to help local officers tackle the problem.

Together with the US Postal Inspection Service, they examined parcels being sent abroad via the Nigerian Postal Service and delivery companies.

A similar operation a few years ago found that 70 per cent of all Nigerian mail passing through JFK airport related to scams.

This latest Nigerian operation uncovered evidence of a vast fraud industry, churning out fake bank drafts, legal documents, cheques and identity papers and hiding them from scanners between sheets of carbon paper.

Raids on addresses in the US, Canada, Netherlands, Spain and the UK followed.

A source said: "This was aimed at tackling the people at the top.

"There have been a number of arrests in Nigeria and the authorities there have been active in tackling this fraud. We believe we have landed a significant blow on the individuals behind this fraud."

Soca is due to reveal further details today of how they thwarted attempts to con UK victims out of millions of pounds.

It's a good start. But Dutch-based investigators Ultrascan believe there are a quarter of a million 419 conmen operating in Nigeria.

They will only stop when people stop sending them.

Here is the URL of the piece for as long as it is good:

<http://www.mirror.co.uk/news/investigates/2007/10/04/multi-billion-fraud-gangs-are-nailed-89520-19893050/>

24 SEP 2007

From ThisDay, a Nigerian newspaper:

FBI Conducts Training for EFCC Officials

The U.S. Federal Bureau of Investigation's (FBI) Legal Attaché Office (Legal) has completed a three - week Law Enforcement Training for 150 members of EFCC, a statement said yesterday.

The statement from the U.S Embassy in Abuja, said that the training was conducted from Sept 3 to Sept.21, dealing with topics of Financial Fraud, Major Case Management, and Interviewing and Interrogation.

It stated the training was designed to provide effective international law enforcement training to Nigeria and to assist members of EFCC to successfully combat and prevent terrorist acts.

"The programmes seek to strengthen and enhance police cooperation by training international police officers to identify terrorists and other organised crime groups, track financing, and use intelligence information to prevent acts of terrorism," it stated.

Mr Ron Nolan, one of the instructors, said "Our job is to work with the Nigerian law enforcement officers and offer them tools that will assist in their job of identifying, disrupting, and dismantling those criminal organisations that are threats to both countries.

"He noted that EFCC was a qualified recipient for this kind of bilateral training, adding that the partnership between it and the agency would benefit both countries in the protection of the lives of citizens.

The statement quoted Mr Ibrahim Lamorde, EFCC Director of Operations, as saying that "The EFCC has received tremendous support from the U.S. government both operationally and in capacity building.

"He pointed out that the assistance was borne out in the work that the Commission had been doing to ensure that Nigeria was no longer a safe haven for fraudsters, corrupt public officers and sundry criminals.

"These efforts are geared toward making our country a more responsible member of the international community. The invaluable support of the U.S. government through her relevant agencies is appreciated," Lamorde said.

Here is the URL of the article for as long as it is good:

<http://www.thisdayonline.com/nview.php?id=90282>

16 SEP 2007

From the Daily Independent, a Nigerian newspaper:

Fake pastor dupes foreigner, arrested

By Andrew Utulu, Reporter, Lagos

A suspected fake pastor, Smith Isong, has been arrested and detained at the Zone 2 Police headquarters, Onikan, Lagos for allegedly duping a foreigner of N3.5 million, using the name of Redeemed Christian Church of God (RCCG).

The suspect, who operated as Pastor Patrick Mark, was arrested on Thursday at the Ojodu area of Lagos, following a report by authorities of the RCCG's His Master's Place Parish in Gbagada that some persons were using the parish's name to dupe a foreigner.

The suspect was arrested with three other members of his gang.

Investigation revealed that the suspects allegedly duped a white man based in Dubai who operates a charity organisation.

It was gathered that the syndicate stumbled on the man's address through the internet and requested for his financial assistance, claiming to be representing RCCG, to enable them carry out some charity work in Nigeria.

It was further gathered that payment of over N2 million was made to the syndicate in 2006 and another N3.5 million this year.

The suspects operate two bank accounts, one with a community bank in Akute-Ajuwon and the other in the Magodo area of Isheri, Lagos. It was learnt that the banks became suspicious when Mark started withdrawing money from the accounts, leaving only a balance of N700,000 in the Akute-Ajuwon branch, which had a deposit of over N2 million. The same scenario was also observed at the Magodo bank.

It was at this point the attention of the church was drawn by the two banks to the financial dealings of the suspects.

It was also gathered that based on this, the attention of the Zone 2 police was drawn through a petition from RCCG Headquarters.

The zonal headquarters was said to have detailed undercover policemen to trail the suspected con men who were eventually arrested. They have confessed to being a 419 syndicate.

16 SEP 2007

From Vanguard, a Nigerian newspaper:

Unveiled! Detectives uncover new '419' ploys

by TUNDE AKINGBADE

AMERICAN organizations and concerned individuals last week unveiled a new type of crimes of persuasion, known locally as 419 carried out by Nigerian con men through the use of dogs and their puppies. In this new wave of 419, Nigerian fraudsters are said to be luring prospective and unsuspecting buyers of dogs and lovers of puppies to buy these domestic animals that are non-existing through the internet.

Last year alone the concerned groups, including the Council of Better Business Bureaus, the Humane Society of the United States, the Internet Crime Complaint Centre and the American Kennel Club disclosed that about 700 Americans were defrauded through the sale of puppies on the internet.

For each fraud, the con men reportedly stole between N40, 000 and N300, 000 through the sale of imaginary puppies. According to reports, though some of the fraud may have originated from within the United States, but Nigerian con men were particularly fingered in the ones that originated from overseas. In these schemes to make money from unsuspecting pet lovers, con men are said to have created websites indicating that they have puppies for sale.

They use two types of tricks which involve what is being described as overpayment scam in which a fraudster contacts someone and negotiates a price and later sends payment for the animal in form of a cashier's cheque. However, the fraudster would ask the potential victim to return the overpayment through an electronic transfer, back to the fraudster or a third party.

The report by Leslie McFadden added that "the victim eventually learns the cashier's cheque is counterfeit and loses the money he or she was supposed to get for the dog, plus any funds wired to the scammer. If the victim actually sent the dog, he or she won't get it back.

In the case of Nigerian 419 men using pets, the Americans warned on the internet last week that the con artists run advertisements on web sites they specifically created for the ploys and offer purebred puppies - typically English bulldogs or Yorkshire terriers - either free or at a discounted price.

The con artist then claims the animal is free or discounted. They also lie further that the owner is a missionary who has been looking for a new home for the dogs who has been suffering from terrible weather or climatic conditions in her present location or that the dog needed a new home after she was rescued from terrible natural disaster

Unsuspecting victims would then be asked to pay for the shipment or transportation of the dog, payment for inoculation and other fees. When the victims pay for all these, the dogs are never sent and the con men keep asking for more money and they give reasons for the delay in transportation.

419 Coalition note: Nothing really new about pets or animals etc. being used as parts of the "tale" in 419 solicitations. Been going on for years, just one of a virtually infinite number of tales that the 419ers come up with. No matter the tale, it always boils down in the end to advance fee fraud.... but the publicity on the pet tales is welcome nevertheless :)

6 SEP 2007

From ThisDay, a Nigerian newspaper:

Nigeria: EFCC, UK, U.S. Anti-419 Operations Intercept N55bn Postal Scam

A joint postal interdiction operations involving operatives of the Economic and Financial Crimes Commission, the United States Postal Inspection Service and the United Kingdom Serious Organized Crimes Agency has ended in Lagos.

The month long operation which was part of the Global Counterfeiting Financial Instrument Initiative Operation was rounded off on August 16, 2007.

A statement by Osita Nwajah Head, Media & Publicity of EFCC said the exercise is the first multi-national interdiction operation of outward bound packages in the country. It saw agents of the three law enforcement agencies poring through tones of outward bound packages in the pre-exporting mail processing centres of the Nigerian Postal Service (NIPOST) and private courier companies like FedEx, UPS and DHL. The operation produced startling discoveries of how criminal elements operating from the country ship fake documents and counterfeit financial instruments abroad. In several packages were found fraudulent identification and counterfeit financial instruments neatly concealed in carbon paper to evade the sensors of scanners.

In all, 15,129 counterfeit cheques related to advance fee fraud scams were intercepted. They include 6,948 blank cheques and others drawn for the sums of \$145.9 million, Euro 211,077, 218.00, over two million Pounds Sterling and 120,450.00 Canadian dollars.

The combined value in naira is about N55.93billion. The operations opened up new investigation vistas leading to the arrest and prosecution of a number of suspects.

Mike Darvey, who led six other operatives of the UK Serious Organized Crimes Agency to the exercise, described the operation as successful. He also commended the professionalism of the EFCC operatives and promised his country's continued assistance to the Commission.

On his part, Sean Lynch who was at the head of the United States Postal Service team described the operation as an eye opener. He said the exercise has proved that not all Nigerians are involved in the scam. He also commended the efforts of EFCC in combating financial crimes in Nigeria.

Similar interdiction operations were carried out simultaneously in Spain, the Netherlands, United Kingdom, Canada and the United States. The global initiative against 419 scam will climax with an international press conference in Washington DC, to be conducted by Chief Executives of selected law enforcement agencies around the world. The EFCC is one of the agencies invited, the statement pointed out.

Here is the URL of this piece for as long as it is good:
<http://www.thisdayonline.com/nview.php?id=88505>

It was also picked up by the BBC, here is that URL for as long as it is good:
<http://news.bbc.co.uk/go/pr/fr/-/2/hi/africa/6982375.stm>

15 AUG 2007

From The Connection Newspapers, Loudoun, VA:

Man Charged in Money Scam

by Erika Jacobson

A 21-year-old South Riding man has been charged by the Sheriff's Office for his alleged role in a counterfeit check scam known as the Nigerian scam.

Sharveen Sharifaie-Arabi was charged with obtaining money under false pretenses, Thursday, July 9, after a sting was set up in the Prime Mart in Chantilly by the Loudoun investigators, the Fairfax County police department and Western Union. Investigators also found \$2,423,070 in counterfeit checks at Sharifaie-Arabi's house.

In the scam, Sharifaie-Arabi allegedly sent his victims a counterfeit check he said contained extra money that they could keep if they would only send him a money order for the remaining amount, Kraig Troxell, spokesman for the Sheriff's Office, said. "By the time they would send the money order and the check is set to clear in the bank, they would find out the check was fake," Troxell said.

The investigation into Sharifaie-Arabi began at the beginning of August, when personnel from Vanderbilt University in Nashville, Tenn., contacted Loudoun investigators. A student at the university reported she had been scammed out of money when she attempt to rent a room to a South Riding man.

Wednesday, July 8, the Sheriff's Office received another complaint regarding the same South Riding man from a man in Rhode Island. The second victim reported receiving a suspicious check from a man in South Riding, which was sent to purchase a Howard Miller display case on the Web site craigslist.com. The suspect sent a check for more then the asking price of the display case and a letter that asked the recipient to send some of the extra money via a money order to a Western Union located closest to South Riding. The money order was allegedly to pay another individual for moving expenses.

In Thursday's sting operation, Sharifaie-Arabi was told that the extra money had been sent to the Prime Mart convenience store and was taken into custody when he went to pick up the check. He has since been released on a \$3,000 bond.

Troxell said it has been difficult for the Sheriff's Office to respond to reports of similar scams because the scammers typically live overseas.

"This is the first time we've seen the actual alleged scammer in Loudoun," he said. "This is the first time we've been able to make an arrest."

Troxell said potential victims would know if they had been victims of Sharifaie-Arabi's scam because they would have sent checks directly to him in South Riding.

"He was using different names on the checks [he sent], but people were sending their money to him through his real name," Troxell said.

If anyone believes they've had contact with Sharifaie-Arabi, Troxell said they should come forward and contact the Sheriff's Office.

Here is the URL of the article for as long as it is good:
<http://www.connectionnewspapers.com/article.asp?article=86062&paper=67&c>

419 Coaliton comment: It is of interest to note that this gent is not a Nigerian, and also that copycats tend to get caught, especially when operating from within the target country :)

12 AUG 2007

From The Eagle, Bryan-College Station, Texas, sent in by a concerned Nigeian:

Police charge woman in scam

By HOLLY HUFFMAN
Eagle Staff Writer

College Station police ended a seven-month investigation Saturday with the arrest of a 59-year-old lawyer who admitted to participating in six e-mail scams over the past five years, authorities said.

Helen Mayfield told police she was the victim of a common financial scam that generally features a supposed foreign dignitary offering millions in exchange for help. But police, who worked with the FBI on the case, said the College Station woman was a willing participant seeking financial gain.

Mayfield was charged with 12 counts of forgery of a financial instrument after police said she cashed fake \$500 American Express Travelers Cheques at First National Bank, where she had an account.

She cashed 14 checks, according to police. The bank contacted police after a dozen were returned.

Mayfield told police she cashed the checks for a client in exchange for a percentage of the cash. The client, she said, was a West African widow having trouble accessing her late husband's \$15 million fortune.

Investigators discovered she was wiring money to Nigeria, Hong Kong, Taiwan, Ontario, Ghana and the Netherlands. She told police she was involved in six scams since 2002, saying she continued hoping someday to get money she was promised.

Mayfield remained jailed Saturday in lieu of \$240,000 bail.

-Holly Huffman's e-mail address is holly.huffman@theeagle.com.

Here is the URL of the article for as long as it is good:
http://www.theeagle.com/stories/081207/local_20070812052.php

419 Coalition note: Generally, when people are arrested for Cashier's Check 419, which this case appears to be, the charges are ultimately dropped. To make the case, the Government must be able to show that the person arrested Knew that the checks presented were fraudulent,

and that the intent was to defraud the bank. Usually the Government cannot prove this. In many instances, criminal charges like this are triggered by the bank, when they try to get their customer to make up losses to the bank or shortages in the customer's account caused by the bouncing of the bad checks, and the customer either cannot do so or refuses to do so. Then the bank approaches authorities to try and get the matter criminalized to get more leverage on the customer to make up the bank's losses, when in actuality the whole thing is actually a civil matter from the get-go, since the intent of the customer to defraud the bank (if any) is generally not possible for the bank - or the authorities - to prove. 419 Coalition prediction is that these charges will go away, unless there are details of which we are unaware that could indeed prove intent to defraud the bank on the part of Ms. Mayfield. It is not the policy of any the US Government, at any level (state, local, and national) nor is it the policy of any government in the world of which we are aware, including the Nigerian government itself, to prosecute victims of 419, including victims of Cashier's Check 419, which is what this case appears to be.

9 AUG 2007

Sent in by our colleagues Ultrascan in the Netherlands.
Six 419ers arrested for scamming Australian businessman.
In French:

La police néerlandaise fait la chasse aux escrocs par Internet
NEWS.fr TV5.org FRANCE24.com TDG.ch AFP

Par milliers dans le monde, se jouant des frontières et des législations, des escrocs spamment l'internaute par des e-mails proposant un héritage juteux ou l'assurant qu'il a gagné au loto. Aux Pays-Bas, une trentaine de policiers les traquent spécifiquement.

Mercredi, la police annonçait l'arrestation de six escrocs présumés, qui avaient extorqué 1,5 million de dollar (1,1 millions d'euros) à un Australien de 49 ans après lui avoir promis, par e-mail, un contrat commercial juteux de 90 millions de dollars (65 millions d'euros).

"Il s'agit d'une fraude massive utilisant les techniques du marketing", précise depuis Haarlem (centre) Harry Jongkind, coordinateur de l'opération Apollo qui mobilise trente policiers en permanence sur la question aux Pays-Bas.

Surnommée "fraude 419" en référence à l'article du code pénal nigérian qui réprime ce délit, elle est surtout le fait des "réseaux ouest-africains", comme le formule la police. En fait, la grande majorité des personnes arrêtées est d'origine nigériane.

"Toute forme de fraude qui utilise les télécoms : internet, l'email ou le fax, souvent combiné avec l'exigence de payer les frais en avance et avant même de pouvoir toucher le pactole ... dont la victime ne verra finalement jamais la couleur", résume M. Jongkind.

"Cela se fait souvent sur des comptes en banque à l'autre bout du monde, et les escrocs ne se trouvent jamais dans le même pays que leur victime afin de rendre la coopération policière difficile", raconte-t-il.

On ne peut plus classique, l'histoire de la victime australienne correspond à ce schéma : "était-il d'accord pour investir 90 millions de dollars au nom de quelqu'un d'autre ?", lui a-t-on demandé par e-mail.

Il lui a alors fallu avancer de fortes sommes, "comme des frais de notaire", a précisé la police. L'affaire, qui a débuté il y a un an au Japon puis traversé d'autres pays, s'est terminée dans un hôtel d'Amsterdam.

Sentant enfin l'arnaque, l'Australien a prévenu la police, qui a réussi à arrêter six escrocs venus lui présenter une valise pleine de billets en lui promettant qu'elle serait bientôt à lui.

Aux Pays-Bas, depuis le début de l'opération Apollo en octobre, la police a arrêté 74 suspects, saisi à leurs domiciles des listes de victimes et d'adresses-mail ciblées, des ordinateurs et disques durs, de l'argent liquide, des faux billets et documents.

Leur inventivité force l'admiration. Ils reproduisent les sites internet de banques internationales comme ABN Amro, ouvrent des milliers de comptes bancaires sous des noms d'emprunts, créent des entreprises inexistantes en inventant sans cesse les histoires les plus crédibles.

Selon Frank Engelsman, un internaute éclairé qui a monté un site sur le sujet (www.ultrascan.nl), ils seraient pas moins de 2.200 à opérer aux Pays-Bas et 18.000 en Europe.

Quant aux victimes, il y en aurait des millions. "Les victimes ayant porté plainte ont payé de fortes sommes aux escrocs, allant de 8.500 à 2,5 millions euros", selon la police.

L'argent récupéré permet ensuite de financer la "fraude bancaire, le trafic de drogue et la prostitution", selon M. Jongkind.

Les policiers néerlandais, qui n'ont pas les moyens de traquer les escrocs sur leur terrain de jeu, Internet, espèrent surtout "rendre les Pays-Bas moins attractifs".

"Cela ne règle pas le problème car il suffit d'un téléphone et d'une connection internet pour reprendre leur activité de l'autre côté de la frontière", concède cependant M. Jongkind.

Autre problème : selon la police, seul 10% des victimes se manifeste.

"La plupart des arnaques ne sont jamais déclarées, soit parce que les gens, un peu honteux, ne vont pas voir la police, soit parce qu'au commissariat on leur fait comprendre qu'on a d'autres soucis qu'une +petite+ escroquerie de quelques centaines d'euros, ce qui constitue la majorité des cas", déplore M. Engelsman.

7 AUG 2007

\$330K RECOVERED MONEY REPATRIATED IN GHASEMI CASE

FAMOUS 419 CASE SUCCESSFULLY RESOLVED

Dr. and Mrs. Shahla Ghasemi of Tampa, Florida announced today that \$330K of recovered 419 losses have been repatriated. The repatriated monies were electronically transferred directly into their bank account by the Central Bank of Nigeria.

The Ghasemi case was one of the most famous 419 cases over the last several years, and received widespread media coverage.

As many will recall, the Ghasemi case is the one in which the Central Bank of Nigeria, at a major event in New York in 2002 attended by former Nigerian President Obasanjo, announced publicly with great fanfare that their six-figure losses had been recovered and were being repatriated. [See 419 Coalition 6 JUN 2007 News for recent developments in the case; 12 DEC 2000 News for a description of the case itself; and 26 and 29 SEP 2002 News for information on the Recovery and Repatriation announcement made by Central Bank of Nigeria. Also see the following News items (among others) for more News on the Case: in 2002 News - 31 JUL, 1 APR, 19 APR, 1 AUG, 10 AUG, 30 SEP, and 8 Oct 2002. There have been articles and comments on it in our more recent News sections as well.]

However, in the years between 2002 and the present, CBN kept coming up with an endless array of silly and unfounded excuses as to why the recovered funds could not be repatriated as promised.

This year at the urging of noted German 419 activist Frieda Springer-Beck, who lives on site in Nigeria, the Deputy Director of the Nigerian Economic and Financial Crimes Commission (EFCC) Mr. Ibrahim Lamorde took a Personal interest in the case. The Director of the EFCC, Mr. Nuhu Ribadu also looked into the matter personally, as did an agent of the US Secret Service onsite in Nigeria. The end result was, as given in the headline above, that Central Bank of Nigeria FINALLY repatriated monies to the Ghasemis in the amount of the monies recovered (though apparently no interest was paid on these monies CBN had ostensibly been holding for five years - perhaps CBN will send the interest along shortly).

Dr. and Mrs. Ghasemi thanked Director of the EFCC Nuhu Ribadu and Deputy Director Ibrahim Lamorde for their efforts in this matter. They also thanked Frieda Springer-Beck for her years of hard work on their behalf, and the Secret Service for assisting them in the final phases of the repatriation process. Finally, they thanked the 419 Coalition, a counter-419 educational NGO, for their six years of guidance in the handling of this case.

However, it was the determination and the tenacity of Mrs. Ghasemi which ultimately brought the case to a successful close.

4 AUG 2007

From the Nigerian newspaper The Punch:

Nigerian arrested in Delhi for internet scam

By Agency reporter

A Nigerian, Okhai Prince Albert, has been arrested in New Delhi, India for alleged involvement in an international internet scam.

A report by the Indo-Asian News Service said Albert, who was arrested on Wednesday, allegedly ran the scheme with his accomplices from Nigeria. He was arrested for allegedly duping an Indian of Rs.650,000 (N2.05 million), Delhi Police said on Thursday.

The report stated that Albert, who is staying illegally in India, was arrested at the Ashoka Hotel in Chanakya Puri after he had gone to collect more money from his victim, Khozaima Gabu, a resident of Ratlam in Madhya Pradesh.

The incident came to light after Gabu registered a complaint with the economic offences wing of Delhi Police. Gabu told the police that he had received an e-mail few months ago saying that he had won a lottery of Rs.20m (N63m); and that to claim the amount, he had to deposit a sum of Rs.50,000 (N157,722) as bank transfer fee in an Icici Bank account of one Prabal Ray Pradhan.

After depositing the amount, he received another e-mail asking him to deposit Rs.122,651 towards taxes. In total, he deposited Rs.650,000 as demanded through a series of e-mails.

The victim was asked to approach the South African High Commission in New Delhi to collect his jackpot. However, outside the high commission, Albert demanded more money from him. The Nigerian asked him to come with money to the Ashoka Hotel within two days.

Deputy Commissioner of Police Prabhakar said, "But Gabu approached the police and a trap was laid at the hotel to nab Albert. During interrogation, Albert confessed to his involvement in an international internet scam and said he had transferred all the money to his accomplices in Nigeria. Further investigations are underway."

19 JUL 2007

A concerned Nigerian wrote in and advised us that NBC Dateline did a 2 part piece on ID theft which also deals with certain aspects of 419 operations. The second part 22 JUL at 8PM EST US time. Here is the URL of a transcript of the pieces for as long as it is good:
<http://www.msnbc.msn.com/id/17938789/>

17 JUL 2007

In from our friends at FraudAid.org:

'I Go Chop Your Dollar' star arrested

Nigerian comedian and actor Nkem Owoh was one of the 111 suspected 419 scammers arrested in Amsterdam recently as part of a seven month investigation, dubbed Operation Apollo.

Owoh became a well known star within the Nigerian film industry, sometimes colloquially known as Nollywood because of its trite plots, poor dialogue, terrible sound, and low production standards.

Owoh starred in the 2003 film Osuofia, and a year later was one of several actors temporarily banned from appearing in movies by Nigeria's Association of Movie Marketers and Producers because he demanded excessive fees and unreasonable contract demands.

Owoh became internationally known for his song "I Go Chop Your Dollar", the anthem for 419 scammers ("Oyinbo man I go chop your dollar, I go take your money and disappear 419 is just a game, you are the loser I am the winner" etc.), which was banned in Nigeria after many complaints.

The song was the title track from the comedy, The Master, starring Owoh as a scheming 419er.

The alleged scammers are suspected of running a series of lottery-based (AKA 419-lite) scams.

419 Coalition Note: Nkem Owoh (Osuofia) was released as soon as his papers were found to be in order, as were many others of the initially detained. As of the end of JUL there were only about 30 of those detained still in custody awaiting trials and/or deportation.

12 JUL 2007

From Sahara Reporters (saharareporters.com):

The UBA Money Laundering Case-Settlement with US Attorney
By Sahara Reporters, www.saharareporters.com

U.S. ANNOUNCES AGREEMENT WITH UNITED BANK FOR AFRICA MICHAEL J. GARCIA, the United States Attorney for the Southern District of New York, today announced an agreement (the "Agreement") resolving the criminal liability of UNITED BANK FOR AFRICA PLC ("UBA") relating to UBA's obstruction, between 2000 and 2004, of the Government's criminal and civil investigations into money laundering of fraud proceeds through accounts held at UBA, including an account in the name of Zamora Nigeria Limited ("Zamora"). The Government civilly forfeited more than \$5 million in fraud proceeds from that account in December 2003. The Agreement provides that UBA will not be prosecuted for any

crimes (except possibly criminal tax violations) related to participation in obstructing the criminal and civil investigations. The Agreement further provides that UBA will forfeit \$5,334,331, representing proceeds of fraud laundered through a Zamora account at UBA, and that UBA will continue to cooperate with the Government.

UBA's Offending Conduct

UBA acknowledged, in a statement of facts that is part of the Agreement entered into today, that it took the position, in response to inquiries made by the Government in both civil and criminal investigations, that UBA and Zamora were unrelated, independent entities. In support of that position, UBA intentionally created and then supplied to the Government certain fake, backdated documents, which had the effect of substantially obstructing the Government's investigations. Specifically, in 2000, after being informed of the Government's investigation, UBA created and produced to the Government certain phony, backdated letters purporting to reflect the resignation in March 1998 of an individual who was actually on the payroll of UBA from 1997 until 2000, and who simultaneously held the position of General Manager at Zamora between March 1998 and 2000. During the same time period, UBA and Zamora in fact had a close financial and business relationship: among other things, expenditures and personnel actions of Zamora were routinely approved by UBA officials.

The Original Government Investigation

In or about late 1999, the United States Attorney's Office and the United States Secret Service began a civil forfeiture investigation into possible money laundering through the Zamora account, which account was opened in UBA's New York, New York branch in March 1998. The Government alleged that the account had been used to launder the proceeds of fraudulent activity. In January 2000, the Government seized, and in 2003 ultimately forfeited, in excess of \$5 million from that account, on the grounds that the Zamora account had been used to facilitate the transmission of at least that amount of the proceeds of various fraud schemes in which victims were fraudulently induced to send monies to Nigeria. In turn, those funds were restored to victims of various fraud schemes. Shortly after the commencement of the civil case, a grand jury in the Southern District of New York began a related criminal investigation. The Government issued subpoenas and official requests for information to UBA in connection with those investigations, seeking to learn what relationship, if any, existed between UBA and Zamora during the period from 1998 to early 2000. It was in response to those inquiries that UBA asserted, from 2000 to at least 2004, that UBA and Zamora were and had always been separate and completely independent entities. In connection with that claim, UBA provided to the Government the phony, backdated resignation documents described above.

The Investigation by the Central Bank of Nigeria

In 2004, the Central Bank of Nigeria ("CBN"), as a result of its own investigation into the relationship between UBA and Zamora, concluded that UBA had violated various provisions of the Nigerian Banks and Other Financial Institutions Act of 1991 (the "BOFIA"), and imposed upon UBA civil penalties totalling 93 million Naira -- or approximately USD \$700,000. Contemporaneously, several members of UBA's Board of Directors, including UBA's then Chairman of the Board, as well as the then Managing Director of UBA's subsidiary, UBA Capital & Trust, resigned from their respective offices at UBA. Those former directors no longer have any position of control at UBA. The Change in Management and Directorship at United Bank for Africa in 2005 Following the departure of the then-Chairman and the other board members, UBA operated under interim, replacement management until July 2005, at which point UBA merged with another Nigerian bank, which was at the time known as Standard Trust Bank Plc. After the merger, the new, combined bank, operating under a new Board and management and new controlling shareholders, kept the name UBA. It is this new UBA management and new Board with which the Government has negotiated and reached the Agreement.

The Decision to Enter Into a Non-Prosecution Agreement

The Government's decision to enter into the non-prosecution agreement took into account, among other factors:

(1) UBA's cooperation, since the arrival of new management and directorship in 2005, with the Government's continuing investigation, by, among other things:

(a) making and assisting in making available for interview multiple witnesses, both from within the United States and from Nigeria,

(b) providing certain documentation from international locations that the Government would not otherwise have been able to obtain in a

reasonably timely fashion, and

(c) providing detailed explanations for UBA's transactions;

(2) UBA's commitment to continue to cooperate;

(3) UBA's remedial actions, including

-(a) the agreement by UBA's New York Branch, in January 2007, to the entry of a Consent Order (the "Consent Order") with the Office of the Comptroller of the Currency ("OCC") (to which UBA's New York Branch is principally subject for federal regulation and examination) relating to the implementation of reforms of the New York Branch's operations and internal controls to assure present and continuing compliance with the Bank Secrecy Act, which Consent Order includes, among other things, substantial restrictions on affiliate transactions and transactions with UBA insiders such as executive officers, directors and shareholders,

-(b) UBA's undertaking of a detailed and searching review of the New York Branch's internal anti-money laundering controls and operations by outside auditors, consultants and legal counsel, and its adoption of a detailed plan of reforms that UBA has worked to implement and institutionalize, in accordance with the terms of the Consent Order,

-(c) UBA's hiring of a new Compliance Officer for the New York Branch, its addition of three full-time compliance staff to bolster the Branch's compliance capabilities, and its engagement of an independent audit firm to address internal audit and control issues,

-(d) UBA's enhancement of the customer due diligence capabilities of the New York Branch through, among other things, implementation of new, computerized transaction monitoring software designed to track suspicious activity,

-(e) UBA's confirmation that the former Chairman is now divested of any holding of ownership of UBA, and (f) the agreement by the New York Branch, on May 2, 2007, to the assessment by the OCC of a \$500,000 civil money penalty;

(4) the absence of any evidence of similar misconduct by UBA since new management took over in 2005; and

(5) the consequences that a criminal indictment could have upon the ongoing operations and employees of UBA. In light of the above, and after careful balancing of all the factors set forth in the Department of Justice's "Principles of Federal Prosecution Business Organizations," the Office has concluded that criminal prosecution of UBA is not necessary to serve the public interest.

Mr. GARCIA praised the investigative efforts of the United States Secret Service in this case. This investigation is being handled by the Major Crimes Unit of the United States Attorney's Office. Assistant United States Attorney DAVID M. SIEGAL is in charge of the investigation.

Here is the URL of the piece for as long as it is good:
<http://www.saharareporters.com/www/report/detail/?id=350>

22 JUN 2007

From the Anchorage Alaska Daily News:

Anchorage man's part in scheme earns prison time
He defrauded friends, sent cash to Nigeria

By MEGAN HOLLAND
mholland@adn.com

A former minister and oil field engineer was sentenced to 46 months in prison Thursday for losing \$150,000 belonging to his friends, church members and local banks in a fraud scheme.

Bill Allen of Anchorage bilked almost a dozen people for four years before he was arrested in August 2006. Even the judge seemed baffled as to how Allen got sucked into a get-rich-quick scam commonly known as a Nigerian advance-fee scheme.

"Over the years, I've seen a lot of cases," said U.S. District Judge John Sedwick. "In some sense, this is one of the saddest I've ever seen."

In the courtroom, the 61-year-old with no criminal history apologized for his actions. "I had no intention of misleading my friends," he said. "I was stupid."

Allen pleaded guilty in March to one count of bank fraud and one count of trafficking in stolen checks and money orders. He agreed to pay his victims restitution.

Allen began wiring money to overseas banks after he was contacted by former friends from Nigeria, said his lawyer Sue Ellen Tatter. Allen worked in the West African country in the 1970s and 1980s on various engineering jobs, she said.

He left in a hurry after a coup and was owed a substantial amount of money. He claims he was owed more than \$5 million by the oil-rich Nigerian government and private firms, she said.

He was not your typical participant who receives one of the millions of e-mails from Nigerian hucksters and falls prey, she said after the court proceeding.

"He thought they were making good on the money they owed him."

He said people he knew in Nigeria contacted him and told him what he had to do to get the millions owed him. Mostly it involved him sending money to Nigeria for "fees."

The scheme entailed him cashing fraudulent checks sent to him, then wiring an Alaska bank's real money back to Nigeria before the bank discovered the check wasn't legitimate.

In a country with rampant corruption and often dysfunctional systems, that he would be receiving checks from companies he never worked for did not raise alarm bells, Tatter said. He thought it was an element of the unorthodox Nigerian business practices.

Allen believed the checks were real.

The schemers knew how to play Allen, she said, and mentioned religion often in their correspondence, including repeated uses of the word God.

The scheme, though, caught up with him, and soon he was in the hole for a substantial amount of money, still needing more for "fees" -- turning to friends to crawl out, Tatter said. "In the end, he was very reckless and perhaps panicky," she said.

Tatter says Allen never made a dime off the scheme and lost a substantial amount of his own money. Over the four years, he traveled to England and Africa in an effort to kick loose the money he believed he would get -- and use to pay people back.

But assistant U.S. attorney Karen Loeffler said greed drove Allen. Why he traveled and whether he got any money from the fraud is an open question, she said.

Twice Allen was contacted by federal law enforcement authorities over the bad checks and was told the whole thing was a scam, she said. But still he kept trying to cash them. In the end, the Secret Service, the FBI and the IRS concluded he tried to cash \$500,000 worth of fraudulent checks.

"He had warning after warning after warning, but he kept doing it," Loeffler told the judge. Allen even bamboozled close friends. Ronald Cupples told his story in court Thursday.

Cupples considered Allen such a dear friend he named two of his children after Allen and his wife. In 2004, he lent Allen \$20,000 because he trusted him, Cupples told the judge, choking up, pausing to gain his composure. "I was badly used by a friend," he said.

When it was Allen's turn to speak, he turned around in his orange-prison jumpsuit to face his former friend in the audience. He looked him in the eye and said he was sorry. "I definitely don't like how I hurt my friends."

The judge recommended Allen do his time in a prison camp in Oregon.

Scams like the one outlined in Allen's case are all over the Internet, and often originate in Nigeria, said Frank Wake, an investigator with the federal public defender office who has investigated previous ones involving Alaskans. People do fall for it, he said. It is one of the country's largest sources of income.

Here is the URL of this article for as long as it is good:
<http://www.adn.com/news/alaska/crime/story/9055215p-8971208c.html>

20 JUN 2007

Paula Zahn of CNN did a piece on Extortion 419 tonight on her show. Of course, Extortion 419 is not new, been going on for decades, in fact the State Department has an example of it given in their 419 alert publication linked on our main

page. But it was a good piece in terms of educating the public on that aspect of 419 criminal operations. Thank you, Paula :)

17 JUN 2007

From the Brisbane Times, Australia:

The scam that cost a family \$1.5m

by Georgina Robinson

Steven Baker was nobody's fool. A straight-talking truck driver from Newcastle, he was an honest, hard-working and street smart bloke who would go to great lengths to help a mate.

But as he sat in the Brisbane police headquarters media room yesterday, with hands shaking, voice hoarse and eyes moist, he must have wondered what had gone wrong along the way.

Was it stupidity or greed that saw Mr Baker and his family were fleeced of \$1.5 million by a startlingly elaborate version of a Nigerian 419 money scam?

It was a question he had probably asked himself many times over since his life started to unravel a year ago.

Over 18 months, Mr Baker was progressively lured into a swindle covering three different European countries and sucked into a whirlwind of African political intrigue and fake diplomatic officialdom.

"It was just unreal the way they had it all set up," Mr Baker said. "You just didn't know that they were basically playing with you."

Play with him, the swindlers did, and the consequences were devastating.

It began with a simple attempt to help a friend, who was a single mother of five children - one of whom was physically and mentally disabled.

The friend was told about an advertisement in a local newspaper that named her and said her absent father, who had English military ties, needed to get in contact.

A barrage of emails from "solicitors" based in Spain told the woman she stood to inherit more than \$4 million that had been smuggled out of the troubled African nation of Liberia.

Mr Baker was initially sceptical of the contact's authenticity but, after some research, he and four other family members agreed to help their friend.

In return, they would get half of the "inheritance".

Mr Baker accompanied his friend to Europe to collect the money from a "security agency".

The initial upfront sum was \$15,000, which he handed over after seeing proof of the cash.

"They took us to a vault, they showed us a very large trunk that had the money in it," he said.

"It was probably one of the scariest moments I think I've ever felt.

"It felt like walking into a morgue - it was cold, it was eerie, and I don't know whether it was meant to be intimidating or not.

"There were a lot of black men, big men in suits, it felt like you were walking into a mafia room."

Mr Baker was then asked for a further \$45,000 to sort out "transfer and tax problems" with the cash.

During the next 18 months and three separate trips, he met various "government officials" in Spain, Italy and Amsterdam.

The pair visited numerous government offices, complete with armed guards, swipe cards and diplomatic paraphernalia.

A young man even stayed with them for a few days, alleging he was the refugee son of a military general who had fled Liberia during the collapse of the ruling dictatorship, led by Charles Taylor.

The money never came through.

"Every time we'd done what they wanted they came up with something else to the point where there was just nothing left," he said.

At some point, Mr Baker said he knew something was wrong, but his pride and a false sense of hope kept him searching.

"By the time we'd paid 100,000 euros, they'd supply certificates and then it was more money to clear records.

"Once we'd gone so far it's hard to turn back. All the money had come from family you know, so it made it very difficult to turn away.

"You had to keep going and they kept pulling your strings the whole time."

When the Baker family's money began to dry up in Italy, the situation turned nasty.

Mr Baker started challenging his contacts about when the cash would come through and a number of heated arguments ensued between him and the African "diplomat".

Events took a dramatic turn when Milanese police turned up and ordered the pair into hiding.

In a remarkable twist, Scotland Yard had been tipped off about an apparent kidnapping and death threat against the Australians in Italy.

Soon afterwards, Mr Baker gave up and returned to Australia for the last time, bitterly disappointed, ashamed and still reluctant to admit he had been conned.

"It was very hard to come home, to see what had happened," he told reporters, shaking and holding back tears.

"It hurt the whole family and they just had to face what had happened. That was hard."

At least a year went by when Mr Baker struggled with the guilt and shame of what he felt he had made his family endure and, ultimately, lose.

He did not think local police would help if international police forces hadn't and a fruitless approach to the government here convinced him justice was out of reach.

It was only when the Novocastrian saw a recent 60 Minutes story on Nigerian scams that he asked one last time for help.

Queensland Police's computer crime investigation squad had a taskforce on 419 scams established for months.

Their investigations with Mr Baker eventually resulted in the arrest of a man in Amsterdam who is now serving a jail sentence.

However, Mr Baker is unlikely to ever see his money returned and he expects to spend the rest of his life paying off debts to friends, former colleagues and banks.

He moved to Redcliffe recently, seeking a fresh start after a nightmare two years that also saw him divorce his wife.

Asked if greed or pride had played any part in his ordeal, Mr Baker was honest.

"Of course, the money was real, we'd seen it, that was the whole thing," he admitted.

"It was helping out a friend and we stood to gain something as well.

"We weren't going to gain millions or anything like that but it would have made things a lot easier."

However, head of QPS's taskforce, Detective Superintendent Brian Hay, was adamant Mr Baker was a victim above all else.

"They saw an opportunity, he thought he was helping out a friend and he's suffered the price for it," he said.

"It was through good will and an earnest appreciation of an opportunity."
Detective Superintendent Hay said no one was safe from these scammers.

"People take what they see and they read it on face value and if you walk into government buildings, why wouldn't you believe it was legitimate," he said pointedly.

"It's very courageous of Mr Baker to come forward because most people don't want to tell us their story.

"They're embarrassed, they've lost everything, they're humiliated, they feel foolish and there would be no doubt that people would accuse them of being greedy or stupid.

"These aren't greedy people, they're victims. They fell victim to very astute, elaborate, well-resourced cons."

Mr Baker's family was waiting for him at the back of the room when the interviews were over.

They had lost a home, a lifetime's savings and two years of life to the con artists.

Yet you were left with the impression that despite his guilt and embarrassment, Mr Baker was just glad they still had each other.

Here is the URL of the article for as long as it is good:

<http://www.brisbanetimes.com.au/news/queensland/the-scam-that-cost-a-family-15m/2007/06/16/1181414600411.html>

16 JUN 2007

According to our colleagues Ultrascan in the Netherlands up to 111 419ers were arrested in Amsterdam this date. Here is the URL of streaming video (in Dutch) showing some of the arrests for as long as it is good:

http://www.at5.nl/speler_at5nieuws.asp?newsid=27424

6 JUN 2007

419 Coalition has received an update on the Ghasemi Case from a usually reliable source. As many will recall, the Ghasemi case is the one in which the Central Bank of Nigeria, at a major event in New York in 2002, announced publicly with great fanfare that the six-figure losses of the victim had been recovered and were being repatriated. [See 419 Coalition 12 DEC 2000 News for a description of the case itself, and 26 and 29 SEP 2002 News for information on the Recovery and Repatriation announcement made by Central Bank of Nigeria. Also see the following News items (among others) for more News on the Case: in 2002 News - 31 JUL, 1 APR, 19 APR, 1 AUG, 10 AUG, 30 SEP 2002, 8 Oct 2002. There have been articles and comments on it in our more recent News sections as well.]

Central Bank of Nigeria already had in its possession, as of 2002, the monies that were to be repatriated to the Ghasemis, according to their public announcements at the New York conference that year.

But to date, the recovered monies have never been repatriated to the Ghasemis. In the time between 2002 and the present, CBN has come up with an endless array of silly and unfounded excuses as to why it can not repatriate the recovered funds as promised.

The Nigerian Economic and Financial Crimes Commission (EFCC) has taken an interest in the Ghasemi case over the last year, with the Director Nuhu Rubadu and the Deputy Director Ibrahim Lamorde looking into the matter personally at the request of German activist Frieda Springer-Beck and the Ghasemis.

That's the background, here is the "new" News and it is a Shocker:

Over the last several months, the EFCC has gradually stripped away all the excuses Central Bank of Nigeria had been giving for not repatriating the recovered funds. CBN finally agreed to repatriate the recovered monies. But when it went to do so.... guess what.... the monies weren't there! That's right, these monies that were supposedly in the safekeeping of CBN since 2002 had just evaporated into thin air! CBN said it could not be sure, but it thinks that the monies were transferred at some point to Omega Bank (which no longer exists) for some reason or other nobody can recall. But it's not sure. The short version is that when crunch time came for CBN and it was being pressured by the EFCC to repatriate the Ghasemi's money *poof*** the money was Gone!!**

Central Bank of Nigeria is not a regular bank like the one on your local streetcorner. It is Government owned parastatal, sortof like the United States' Federal Reserve Bank or the UK's Bank of England (though it does do commercial banking business directly which the Fed does not, not sure how Bank of England does things). CBN regulates and governs All the banks in Nigeria and is the nation's Official bank. It is the "bank of banks" as it were for Nigeria. For CBN to misplace funds, especially funds that it announced with so much ballyhoo that it has in its possession, is simply Outrageous. That sort of thing undermines the credibility of CBN and the Nigerian government in not just 419 related matters, but in terms of All financial matters, and further leaves CBN open to allegations of internal theft and corruption...

It has been reported by usually reliable sources to 419 Coalition that the EFCC has now told CBN in even stronger terms that it better come up with the money and repatriate it to the Ghasemis forthwith. We here at 419 Coalition concur. If CBN can't find the monies it was safeguarding, it had better come up with funds out of its own pockets to replace them. Or people at CBN need to start going to jail courtesy of the EFCC. Enough is enough....

19 MAY 2007

From the London Times:

E-mail fraudsters: we know where you live

Jack Malvern

Explore the scammers map of the UK [at this URL
<http://maps.google.co.uk/maps/ms?ie=UTF8&msa=0&msid=107177327876601283360.000001123a5ff121cafc4&hl=en&com=1&ll=54.02068,-2.48291&spn=6.236727,14.018555&z=6> r

A map showing the location of British-based fraudsters who extract money from their victims with enticing get-rich-quick schemes has been compiled for The Times by investigators.

Each pin marks the address, to within 100m, of a scammer who makes a living by dispatching e-mails that promise huge financial rewards in return for a small upfront investment.

A typical scam involves someone claiming to be the widow of a wealthy Nigerian politician who needs help to release a multimillion-pound estate. The scammer promises a share of the fortune after extracting a series of fees to transfer the money.

Ultrascan, a Dutch company that specialises in investment fraud, compiled the map from its database of 713 scammers that it tracked down in Britain last year. It estimates that there are 2,120 people running advance-fee frauds in Britain, but they have little to fear from the police because little effort is made to prosecute them.

Even if police had the resources to track fraudsters, they would have to overcome the fact that the victims are nearly always based overseas.

Scammers in Britain, who make an estimated £190 million a year, primarily target victims in the Middle East or Far East, says Frank Engelsman, Ultrascan's specialist in advance-fee fraud.

"Scammers always make sure that their victim is in a different country," he said. "They need you to be a stranger in the country where they are. They need the police not to be able to find the victim." Britons who have received advance-fee fraud e-mails have probably been sent them from Spain, which has an estimated 2,840 advance-fee fraudsters. Advance-fee fraud originated in Nigeria in the 1970s as mail-based fraud and has evolved to take advantage of fax machines and e-mail.

Mr Engelsman estimates that Nigeria is home to 250,000 fraudsters and that most of the 23,740 scammers operating outside Nigeria are of West African origin.

Ultrascan compiles its list of fraudsters by responding to e-mails and posing as people who are ready to part with their cash. It obtains addresses by tracking e-mails and telephone numbers and by arranging to meet members of the fraud ring.

Mr Engelsman said that he was willing to share the database with law-enforcement agencies, but that Britain had a poor record of tracking down advance-fee criminals.

He said that police activity against advance-fee fraud, also known as 419 fraud after the Nigerian criminal code, almost completely stopped in 2006.

The Serious Organised Crime Agency (Soca) and the Metropolitan Police said that they preferred to disrupt 419 scammers by taking down their websites and stopping their internet access.

Mr Engelsman said that closing down cells was often ineffective because fraudsters passed on their victims' details to other cells. "The police can arrest a scammer in Haringey and within hours the victims are addressed by another cell. The victim has no idea that they are being contacted by someone else."

Britons are the second most targeted victims after Americans. British companies and individuals lost an estimated £267 million in 2006, an increase of £5 million since 2005.

The scams

- Maryam Abacha, the widow of the late General Sani Abacha, promises a share of her husband's \$35 million estate if you can help her to retrieve it from a security company in Europe. She is unable to access it herself because of a vendetta against her by the President . . .

- Bakare Tunde appeals for your help in rescuing his cousin, a Nigerian astronaut who is stranded on a secret space station. If you help him return to Earth he will gratefully share his \$15 million fortune in accumulated flight pay. This story was first invented as a satire on outlandish scams, but has since been used by professional fraudsters.

- Isabella Caromel claims to be a terminally ill victim of the Boxing Day

tsunami in 2004 who wants you to help her to distribute her \$10 million fortune to charity . . .

- Sergeant Joey Jones, an American soldier serving in Iraq, claims to have stolen \$25 million from Saddam Hussein's bank account and is willing to give you a third if you help him to move the money . . .

- Cajar Nacional, the Spanish national lottery, informs you that you have won €150 million but must pay a fee to process your winning certificate . . .

= The "Government of Great Britain" has identified you as the next-of-kin of one of the victims of the July 7 bombings, who left an estate of £3.5 million. The money is yours if you provide a fee to release the funds . . .

[Sources: hoax-slayer.com, skepdic.com]

Here is the URL of this article for as long as it is good:
<http://www.timesonline.co.uk/tol/news/uk/crime/article1811228.ece>

17 MAY 2007

From ThisDay, a Nigerian newspaper:

Money laundering: U.S. delists Nigeria from non-conformist nations

By Ayodele Aminu

The anti-money laundering reforms embarked upon by the present administration through the Economic and Financial Crimes Commission (EFCC), received a boost yesterday as the United States Financial Crimes Enforcement Network (FinCEN) removed Nigeria from its list of countries that are non-cooperative in the fight against money laundering.

This cheery news, which was communicated to banks and other financial institutions operating in the U.S. by Director, United States FinCEN, James H. Freis Jr., is coming barely one year after the Paris-based International Finance Action Task Force (FATF) de-listed Nigeria from the league of Non Co-operative Country and Territory (NCCT).

The FINCEN Advisory reads in part: "This Advisory is being issued to inform banks and other financial institutions operating in the United States that Financial Crimes Enforcement Network (FinCEN) Advisory Issue 32, regarding the Federal Republic of Nigeria, is hereby withdrawn. Since the issuance of Advisory 32, and as reflected in its June 23, 2006 decision, the Financial Action Task Force on Money Laundering has removed Nigeria from its list of countries that are non-cooperative in the fight against money laundering, recognizing the progress Nigeria has made in implementing anti-money laundering reforms."

Justifying its decision, FinCEN noted that Nigeria has enacted significant reforms to its counter-money laundering system, addressing the deficiencies listed in Advisory 32, and has taken concrete steps to bring these reforms into effect. Because of the enactment of new laws and the beginning of effective implementation, the enhanced scrutiny called for in Advisory 32 with respect to transactions involving Nigeria based on its previous listing as a non-cooperative country is no longer necessary.

The US FinCEN however, noted that the withdrawal of Advisory 32 does not relieve institutions of their pre-existing and on-going obligation to report suspicious activity, as set forth in regulations issued by FinCEN and by the federal bank supervisory agencies, as well as their obligation to comply with all other applicable provisions of law.

It would be recalled that the United States Department of the Treasury Financial Crimes Enforcement Network has on April 2002 issued an Advisory to intimate banks and other financial institutions operating in the United States of serious deficiencies in the counter-money laundering systems of the Federal Republic of Nigeria.

In issuing the Advisory, it noted among others that Nigerian law fails to criminalize the laundering of illicit proceeds, other than proceeds derived from narcotics trafficking; Nigerian banks are not required to report all suspicious transactions; banks are exempt from making a suspicious transaction report for any transaction which they decline to conduct or which is discontinued prior to completion. It also noted that there is no penalty under Nigeria's laws for failing to comply with the suspicious transaction reporting obligation, adding that these deficiencies, among others, have caused Nigeria to be identified in June 2001 by FATF as non-cooperative in the fight against money laundering.

But on June 23 2006 the FATF removed Nigeria from the list of countries and territories that are non-cooperative in the fight against money laundering and terrorist financing. The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. Since the de-listing of the country by FATT last year,

Nigeria which had become pariah state in terms of foreign financial assistance when it was listed among the 23 jurisdictions designated as non-cooperative countries and territories has joined the global world.

Before then, the inclusion of Nigeria in FATF's list of non co-operative countries and territories had far reaching implications on the Nigerian financial services sector as foreign financial institutions no longer had confidence in Nigerian, and as such refused

Nigerian banks lines of credit. Most international agencies had downgraded their credit lines to Nigerian banks due to their perception of the risk profile of both the country and its banking industry. The implication of this development was that Nigerian banks had to have to pay upfront for any financial transactions with foreign financial institutions - a development that tended to reduce the amount of financial assistance that ought to have given to local entrepreneurs and industries. These foreign lines of credit are usually with repayment tenors of between 180 days to five years.

But since June 23, 2006 the story has changed as Nigeria continued to record new investment among, which includes the Export-Import Bank of the United States' (Ex-Im Bank) \$300 million (N39 billion) for 14 Nigerian banks to support US exports to Nigeria.

419 Coalition Comment: We're not sure the de-listing is warranted. Victims of 419 are still having considerable trouble tracking stolen funds which were sent to Nigeria, and in getting Nigeria to repatriate recovered funds. In fact, in the Ghasemi case, where the Nigerian Government announced publicly with much fanfare years ago that stolen monies had been recovered, the Ghasemis are still awaiting the repatriation of the recovered funds. Additionally, we call again on the EFCC to release a comprehensive list of to whom recovered funds have been repatriated and in what amounts. From a 419 victim's point of view, it does little good if funds are recovered unless they are being routinely repatriated, and it would behoove the EFCC to be more transparent on repatriations in our view.

15 MAY 2007

The following URL's of videos regarding scambaiting the 419ers were compiled and sent in by a Nigerian concerned about 419 matters. Here they are for as long as the URL's are good:

<http://www.youtube.com/watch?v=gHphszkawoU&mode=related&search=>

<http://www.youtube.com/watch?v=7PVK0R01tRw&mode=related&search=>

<http://www.youtube.com/watch?v=8PQANsFisvU&mode=related&search=>

<http://www.youtube.com/watch?v=eU9WqhCiQ8g&mode=related&search=>

<http://www.youtube.com/watch?v=Z0bt6wnRen8>

<http://www.youtube.com/watch?v=EiCqefRhZdg&mode=related&search=>

<http://www.youtube.com/watch?v=r0t-iaq9nzo&eurl=http%3A%2F%2Fnajaman...>

25 APR 2007

Ultrascan Advanced Investigations in the Netherlands has filed this report:

The Amsterdam police last Monday arrested 5 people and confiscated computers, fake travel documents, bogus banking documents. The suspects are being held by the Dutch authorities pending extradition to the US, where they could face up to 20 years in prison. Probably for wire fraud and mail fraud.

The fraudsters in this scheme allegedly fleeced hundreds of unsuspecting victims from the US, NORWAY, INDIA and GREECE with promises of charitable contributions and personal riches.

This scam ring has members in The NETHERLANDS, BELGIUM, GERMANY, GREECE, SPAIN, ENGLAND, FRANCE, ITALY, CANADA and of course NIGERIA. One can expect more arrests to follow in those countries IF law enforcement sees fit, because in some of those countries addressing Nigerian 419 Advance Fee Fraud is not a priority.

The scams involved fake internet banking and security deposit companies, victims should open an account to see the millions of dollars waiting for them. Or visit a security company to see boxes with fake gold or dollar bills and see the wash wash trick to convince them of the "real deal".

This scam ring is/was active in Europe since March 2003, we estimate

the damages that this scam ring inflicted to victims until today, in the tens of millions!!

419 is the 'world's most successful scam' with losses to victims totalling \$28 billion.

The fraud is spreading rapidly and becoming more sophisticated.

Some of the Fake names and institutions (A.K.A.) used by THIS scam ring:

Gran Manera Offshore Investment Finance
Anchor Security And Trust
Ervigio Express Clearing Services Ltd
Global security
Paul Adams
Religion Clearing house
David Reiman
Central and West Euro Funds Monitoring Unit
Embassy of Ivory Cost in Brussels
the dutch Ministry of Finance
Richard Darwin
Brenda Hoffers

Here is the URL of another report on the same case from The Register, a UK news site, for as long as it is good:
http://www.theregister.com/2007/04/25/another_419_scamring_nicked/

10 MAR 2007

From the Hindustan Times, New Delhi, India:

Indian BPOs feeding 419 scamsters

Pramit Pal Chaudhuri

The 419 scam is going global and hi-tech. What originally began as a lark among students left jobless by Nigeria's 1980s oil bust has become the world's most pervasive financial fraud run by organised mafias.

The 419 scam is best known for the ubiquitous spam offering jobs or money in return for small advance payments that crowd everyone's cellphones and computers. India is becoming increasingly entangled in this network. Besides becoming a target for 419 conmen, India is becoming a hub for 419 fraud activity in two other ways.

First, India is home to an increasing number of rings that operate the fraud in other countries. Frank Engelsman, an expert with the Netherlands-based Ultrascan Global Investigations Unit, says 419 scam rings "try to keep one jurisdiction between the scammer and victim". So rings set up in India will work to dupe people in other countries. Indian victims will be targeted by rings in Thailand or elsewhere.

This year's Ultrascan survey of 419 fraud estimates there were at least seven rings based in India last year, up from three in 2005. The seven rings probably had a little over 100 individual operatives. Engelsman says, "Our view is that these are Nigerian-run operations." The rings are often interlocking, sharing their earnings with each other.

There are a few cases of Indians being duped by a ring based in another part of the country: Kolkatans and small-town Maharashtrians lured to Mumbai to pay for packets of "blackened money" and "chemicals" to clean them.

Second, some small Indian call centres are being used to handle the information gathering that victims are often asked to provide to collect their supposed reward. For example, a call centre will be hired to ask the victim for his name, fax and phone number to lull him into believing these are from a legitimate organization. Engelsman recommends: "Call centres should check if their client and his company really exist. Google the names of both together with the word 'scam'."

The growing Indian nexus reflects a pattern developing in all emerging economies. Governments neglect the issue at their peril. Canada ignored the problem for decades and has now emerged as a major 419 scam hub. The US Secret Service's Michael Sameremetis says, "A large part of the scamming in the US is coming out of Canada." His service is the lead US agency handling 419 fraud. Engelsman adds, "One ring in Canada has been there for five years and is now the biggest in the world outside Nigeria."

One of the signs of the crime's evolution is how adept scammers have become at duplicating official documents and entire websites. At one point, 419 fraudsters had 10 copies of the Royal Bank of Canada website in the Internet to induce payments from victims.

Police agencies are not immune. A fake Interpol site pops up regularly every year around November, says one fraud expert. The Secret Service has warned that 419 scammers are sending emails claiming to be from the agency. Victims have been known to call fake police sites and been told by "policemen" that the fraud offer is genuine. One such fake site, of the Filipino equivalent of the FBI, www.nbigov.com, is still on the Internet.

A post-9/11 twist: 419 victims are told their payments are being held up for "terrorism clearance certificates" and fees should be paid to a fictitious government anti-terrorism agency.

Here is the URL of the piece for as long as it is good:

http://www.hindustantimes.com/news/181_1948275,0002.htm

419 Coalition comment: Nobody is actually sure of how 419 got started during the 1980's in Nigeria, but attributing it to some students having a lark seems a bit simplistic to us. Also, while the USSS Agent is certainly correct that a large part of scamming in the US is coming out of Canada, we here still see Most of the 419 Scamming in the US coming out of Netherlands, UK, Nigeria, and South Africa.

9 MAR 2007

From the Hindustan Times, New Delhi, India:

US to find means to stop spread of 419 fraud

Pramit Pal Chaudhuri

Alarmed at the number of US citizens falling victim to the Nigerian 419 scam, the US State Department last month issued a warning brochure. The US consulate-general in Lagos can receive 3,000 inquiries from victims a year, says the pamphlet "International Financial Scams".

In its commonest form the 419 fraud, a common part of everyone's spam email and SMS, dupes a victim to send a small amount of money to a fake bank or law firm in return for a promise of marriage, a job or simply more money.

The US is the most lucrative 419 market, with losses in 2006 estimated at \$790 million, a 10 per cent increase over the year before, says a report by the Dutch-based firm Ultrascan Advanced Global Investigations. The UK comes second with \$530 million.

The State Department brochure reflects standing US policy that the solution is education. Says Michael Sameremetis of the New York office of the US Secret Service, the lead US agency assigned to tackle 419, "The way to stop this is to educate the public as much as possible."

An expert on Ultrascan's 419 Unit, Frank Engelsman, says education and working with internet and cellphone service providers are the two commonest anti-419 tactics of governments. "These are low-cost approaches. The problem cannot be solved with existing law enforcement methods."

Indians are in a particularly sorry state. Ultrascan, though it is a private firm without policing authority, receives pleas for help from dozens of desperate Indians every year.

One man from Kolkata emailed them recently about being defrauded by a "pastor" in Senegal seeking money to help a "girl in a refugee camp" to retrieve "her father's money" from a UK bank. Taken in by carefully fabricated Standard Chartered Bank documents, the victim lost \$9,750. "I seek your help," he emailed Ultrascan.

Many people dismiss those who fall for 419 ploys as victims of their own greed. However, many 419 scams today exploit humanitarian instincts. Engelsman says many fraudsters "prey upon people's altruistic impulses". They pepper their conversations with references to god, often targeting religious people.

"The 419 scam industry uses the same human characteristics to sell its lies and myths as do all religions," says US author Brian Wizard, who wrote a novel "Nigerian 419 Scam: Game Over!" based on his personal experiences with these conmen.

Ultrascan advocates a centralised, "victim-friendly" system that has a reporting and researching centre run by an NGO as its primary feature. The centre, in turn, can provide information to the police needed for arrests. Canada's "Phonebusters" programme comes closest to this model.

There is little evidence educational drives or software-based solutions

by themselves are effective. Samerentis admits, "We find it perplexing that so many people continue to hand over money to people they have never met

Email author: pchaudhu@hindustantimes
Here is the URL of the article for as long as it is good:
www.hindustantimes.com/news/181_1947319,00050001.htm

7 MAR 2007

From the Hindustan Times, New Delhi, India:

India an emerging market for Nigerian fraudsters

Pramit Pal Chaudhuri

The world's most widespread financial fraud, the Nigerian 419 scam, is finding new pastures in Asia. India is the third fastest growing market with the defrauders' earnings from Indians increasing nine-fold in one year, says a report by the Dutch firm Ultrascan Advanced Global Investigations.

Almost every cellphone and email user has been solicited by a 419 con man. The best-known ploy is a message claiming there are unclaimed fortunes in banks that can be accessed if someone puts up a little money upfront.

The '419' label refers to an outdated clause of the Nigerian Criminal Code covering such crimes. Among experts, this and variations of the same scam are known as 'advance fee fraud.'

The report estimates losses by Indian firms and citizens from the fraud totaled \$32 million in 2006, up from \$3.5 million in 2005.

This is small potatoes compared to the \$3.88 billion the report, issued in late January, says the fraud raked in last year worldwide. But the growth figures are in Asia. Dubai, where the take from victims increased by a factor of 34 times, is the fastest growing market. Dubai was followed by Thailand, India and China.

South Asian businessmen are among the Dubai victims. A common bait: fake multimillion dollar cement contracts linked to the Persian Gulf port's construction boom.

Frank Engelsman, who has been tracking the organised gangs behind the fraud for 12 years for Ultrascan, says the defrauders tend to track 'new email connections in India in order to target the not yet internet savvy.' Based on the complaints his firms receives from India, most of the victims are 'older Indians from smaller cities and villages.'

The 419 defrauders have developed dozens of different methods to ensnare the gullible.

Offers of romance are used in the West. A State Department brochure on 419 con schemes issued a fortnight ago calls this scam 'Gorgeous People in Trouble.' Other varieties offer lottery winnings and legacies from long-lost relatives.

Says Engelsman: "My personal experience with 419 victims from India is that 'employment,' 'being successful,' 'improve yourself by learning fast' and 'luck' are related to the scams they fall for."

Ultrascan calls 419 the 'world's most successful scam' with losses to victims totalling \$28 billion. 'Our estimates are very low ones,' warns Engelsman. The fraud is spreading rapidly and becoming more sophisticated. 'The worst part is the sorrow, murders, suicides and long-term suffering of the many victims, which sometimes means whole villages or collectives.'

Email author: pchaudhu@hindustantimes
Here is the URL of the article for as long as it is good:
www.hindustantimes.com/news/181_1946489,00050001.htm

1 MAR 2007

The US State Department has released a new brochure on Financial Scams. It is very good, in our opinion. Here is the press release on the brochure, and we have put a link directly to the entire brochure on our main page as well:

New International Financial Scams Brochure

The Bureau of Consular Affairs (CA) has issued an International Financial Scams Brochure to help Americans identify and avoid financial scams originating from overseas. It is available at:
http://travel.state.gov/pdf/international_financial_scams_brochure.pdf.

The Bureau of Consular Affairs' Office of Overseas Citizen Services receives daily inquiries from American victims and potential victims of international financial scams. In some cases, Americans have been defrauded of thousands of dollars. Internet dating, inheritance, work permits, overpayment and money laundering are a few of the scams most recently reported to U.S. Embassies around the world. The International Financial Scams Brochure provides full detailed descriptions of the often sophisticated

scams reported to U.S. Embassies and Consulates abroad, and includes samples of email messages and offers that have been sent to potential victims. As illustrated by the brochure, the perpetrators often prey on potential victims' goodwill by fabricating increasingly complicated but believable scenarios.

Americans concerned that they may be the victims of an international scam may call the U.S. Department of State at (888) 407-4747 or the nearest U.S. Embassy or Consulate. Victims of international financial scams may also report their concerns directly to the Federal Bureau of Investigation (FBI) at <http://www.ic3.gov/> [2007/147]

18 FEB 2007

This was sent in to us as having appeared in a Nigerian newspaper, but unfortunately we can't find where it appeared, so here it is with that proviso:

Undergraduate bags 26 years jail term for Internet fraud

A 24 -year-old Internet fraudster, Mr. Silas Stephen Uwem, has been sentenced to 26 years imprisonment.

Justice Tijani Abubakar of the Federal High Court in Lagos, convicted Uwem for operating a bank account with the Access Bank Plc that suggested money laundering of illegal funds.

The judge also ordered that the N16m, found in the bank account of the convict, should be forfeited to the Federal Government.

A certified true copy of the judgment was exclusively made available to our correspondent in Lagos on Friday.

The convict was given two years on each of the 13-count charge that was preferred against him by the Economic and Financial Crime Commission.

His sentence would, therefore run concurrently from the date of his arrest while the convict would actually serve two years behind bars.

Uwem, an undergraduate of the Lagos State University, Ojo, was said to have a total lodgment of N16m in Access Bank, which he reportedly admitted was obtained through Internet fraud.

The convict also allegedly stated that he belonged to a syndicate of Internet fraudsters that specialised in duping people through Western Union Money Transfer.

Uwem further claimed that he received several sums of money by internet fraud and that part of the N16m at Access Bank was got through chatting on the Internet with foreign nationals.

His alleged earlier claim that his father also gave him part of the said N16m was refuted by his father, who told the EFCC that he only gave his son N250,000.

Convicting Uwem, Justice Abubakar held that the accused was guilty as charged. He said that his transferring and lodgment of various sum of money into his Access Bank's account no 0081510014704 with the aim of disguising the origin of the money was an offence that was contrary to Section 14 (1) of the Money Laundering Prohibition Act, 2001.

The judge added that he took into consideration, the convict's age and his status as an undergraduate during the allocutus (plea for leniency) before sentencing him.

Justice Abubakar stated, "I order that the amount (N16m) currently held in the convict's account No. 0081510014704 at the Access Bank Plc be forfeited to the Federal Government of Nigeria.

"The convict is also warned to be a better person after serving his prison term."

The convict was arrested on May 4, 2006 at the bank's premises when he went to the bank to bail his friend, Aifuwa Umweni, who had earlier been arrested by the bank officials for attempting to fraudulently withdraw money from the convict's bank account.

When interrogated by the bank officials, Umweni allegedly confessed that he lived in the same house with the convict.

But the convict later confessed that he did not authorise Uwem to withdraw from his account.

Uwem, who is also a teenager, was also discovered to allegedly have N5m in his bank account with Access Bank and that he was also an internet fraudster.

The bank later transferred the convict to the EFCC for further interrogation.

The anti-graft body consequently brought Uwem to court on October 12, 2006 and he pleaded not guilty to the 13-count charge.

The accused later filed a bail application and the court granted him temporary freedom on January, 31, 2007. [see related article from the Daily Sun, also 18 FEB, below]

419 Coalition comment: In this article, it says that the Judge has ordered that the recovered 419ed monies be "forfeited to the Federal Government of Nigeria." We hope that there is some missed communication or somesuch here, as any assertion that recovered 419ed monies should somehow belong to the Government of Nigeria is Outrageous. The 419ed monies belong to those who it was 419ed from, period. The Government of Nigeria is certainly not entitled to willy-nilly keep recovered 419 funds. That, from a victim's point of view, would make the Government of Nigeria just as much a thief as the 419er was who stole the money in the first place. Let us hope that what the judge really meant is that the recovered 419ed monies were to be turned over to the Government of Nigeria for repatriation to the victims of this 419er, that would be a proper ruling.

18 FEB 2007

From the Nigerian newspaper, the Daily Sun:

INTERNET RATS: They have N23 million in their accounts, being proceeds from wire fraud

A father of two young men recently got the shock of his life when he discovered that despite the fact that his family was wallowing in poverty, his sons were millionaires.

The man, Mr. Silas, was arrested by the Economic and Financial Crimes Commission (EFCC) when operatives of the commission picked up his sons, Silas Stephen Uwem and Silas Aniekan for having N23 million in their bank accounts.

Unknown to their father, who lives in a one-room with his family, his sons and their friends were raking in millions of naira from internet fraud.

The cat was, however, let out of the bag when, on Friday, May 5 2006, Aniekan went to a Lagos-based bank to make a withdrawal of N5,000 from his account.

When the application was processed, it was discovered that he had less than N1,000 in the account.

Aneikan allegedly got another form for a withdrawal from another account belonging to his friend Kennedy Aifuwa.

Posing as the real owner and having supplied the account number correctly, the teller officer noticed that he had seen him earlier. A thorough check of the mandates of the account was conducted which was at variance with the information supplied by Aniekan.

It was at this stage that the bank officials suspected a foul play. The bank conducted a close check on the account and discovered that it had a lodgment turnover of over N5 million and the owner of the account, Kennedy Aifuwa, was contacted.

Aifuwa, contacted Aniekan's elder brother, Silas Stephen and both of them went to the bank. Unknown to them, the bank had alerted operatives of the EFCC.

A source at the commission said: "They walked straight into our net. The suspects tried to compromise the bank officers through tips to get Aniekan off the hook. Their overtures became more suspicious when they discovered that Silas, 26, has an account with the bank with a lodgment turnover of over 18 million. We also discovered that Aniekan was not as successful as others."

Painstaking investigations revealed that the three suspects were Internet fraudsters popularly known as "Yahoo Yahoo boys."

On getting to the premises of the commission, Stephen claimed that the account which had over N18 million belonged to his father. The old man was contacted and he confirmed that the account was his. He told the investigators that the highest amount he had ever lodged in the account was N200,000. when he heard that his son had over N18 million in the account, he screamed: "Stephen, you mean you have so much money and we are wallowing in poverty."

When Stephen realized that the game was up, he sought to plead bargaining with Justice Abubakar Tijani of the Federal High Court, Ikoyi, where Stephen was charged on a 14-count charge bordering on money laundering and internet fraud. While delivering judgment, the judge said the 28-year jail term would run concurrently, while the convict also forfeited the balance in his bank account.

While Stephen has been convicted, his two accomplices, Aniekan and Kennedy, are still standing trial.

Here is the URL of the article for as long as it is good:
<http://www.sunnewsonline.com/webpages/features/crimewatch/index.htm>

16 FEB 2007

From the Eugene, Oregon Register-Guard:

Man seeking love finds Nigerian scam

By Rebecca Nolan

A 55-year-old Eugene man looking for romance became an unwitting participant in an international scam to ship goods purchased online with stolen credit cards to Nigeria via Europe.

Dubbed the "Nigerian repackaging scam" by law enforcement, the scheme aims to bypass restrictions of overseas shipping companies such as FedEx, DHL and UPS - which limit shipments to west Africa because of pervasive fraud - by finding gullible Americans to serve as intermediaries.

The victims receive the stolen goods - often unaware of their origins - and send them on to Europe, where other scammers receive and ship them to Nigeria, Eugene police financial crimes Sgt. Terry Fitzpatrick said.

The scammers usually promise to reimburse the Americans for their shipping expenses, but the money never arrives.

Despite years of warnings about similar schemes - many involve people claiming to be from Nigeria - people continue to fall for the scams, often losing thousands of dollars in the process.

"It's one of two things - either they're very, very naive or they're very greedy," Fitzpatrick said. "Some people want to get something for nothing. The old adage, 'If it sounds too good to be true, it probably is,' really applies in these cases."

The Eugene victim was lured into the scheme by a woman he met on the Internet, Fitzpatrick said. They struck up an online friendship, and soon the woman was talking about marriage and moving to Eugene to be with him.

Eventually she asked the man to help her send some packages to England. Smitten, he agreed, and she provided instructions for repackaging the goods and sending them on to Europe, where many companies are more lenient about shipments to Nigeria.

An online retailer based in Austin, Texas, alerted local investigators to the scam before the Eugene man completed a shipment, Fitzpatrick said. The man, who lives in the Barger Drive area, allowed Eugene detectives to read his e-mail correspondence with his would-be sweetheart and fully cooperated with police.

Fitzpatrick sent the case on to the FBI, which has investigated similar international scams in the past. At a recent fraud symposium, an FBI agent showed slides of warehouses in Nigeria stocked with computers, microwaves and other electronics stolen and shipped the same way, Fitzpatrick said.

Scammers find their victims on the Internet or through "Work at Home" advertisements.

"They offer you a job repackaging and mailing things for, say, \$6,000 a month," Fitzpatrick said. "After you mail a whole bunch of things, they send you a check and, of course, it's bogus."

People often go several months before they realize they've been had, he said.

"We're just hoping to get the message out there so more people don't get victimized," he said.

Here is the URL of the piece for as long as it is good:
<http://www.registerguard.com/news/2007/02/16/cl.cr.scam.0216.p1.php>

8 FEB 2007

This in from our associates Ultrascan in the Netherlands:

Today 21 West African 419 advance fee fraudsters were arrested in Amsterdam south east (Bijlmer).

The arrests were carried out by the "Apollo" team of the Dutch Federal Police fraud section.

9 of those arrested were in the Netherlands illegally and were handed over to the department of immigration.

31 JAN 2007

This in from our associates Ultrascan in the Netherlands:

Spanish police arrest 43 Africans on fraud charges

MADRID, Spain: Spanish police have arrested 43 Africans on suspicion of running a fraud ring in which people were duped into paying money as a handling charge to collect lottery winnings.

Authorities estimate the men - 42 Nigerians and one Senegalese - bilked people out of more than €2 million (US\$2.6 million) altogether. They were arrested Tuesday in Seville, and another five Nigerians were arrested for being in Spain illegally, the Interior Ministry said.

25 JAN 2007

From the Nigerian newspaper the Daily Sun:

International conman in EFCC's net

By OLUWATOYOSI OGUNSEYE

A suspected Nigerian fraudster has been charged to court by the Economic and Financial Crimes Commission (EFCC).

The 28-year-old Enyinnaya Nwokefor was arraigned alongside Nnamdi Chizoba a.k.a Yellow Man, Abdul Rahman, Michael Aderson, Edmund Walter, Nancy White, Anthony Friday Ehis a.k.a John J. Smith and Kesandu a.k.a Keke. All the suspects, except Nwokefor, were arraigned in absentia.

It was alleged that the accused and others had between 2002 and 2006 obtained various sums of money running into millions of dollars from several United States indigenes under false pretences.

After convincing the victim that he was real, Nwokefor, in one of the schemes, posed as Eric Williams, a wealthy old man suffering from throat cancer, who needed a trustworthy agent to help dispense \$55 million dollars charity fund to the underprivileged in the US, as he would not be able to travel from Amsterdam to USA.

The scam letter was sent to many persons in America and other countries before they eventually got a victim.

Daily Sun learnt that the suspect, while communicating with his victim always sounded as if he had a throat problem. Nwokefor, then asked his victim to send some money to clear the \$55 million which he said were packed in two boxes.

The suspect initially got \$38,000 through Western Union Money Transfer in Amsterdam. He later convinced the victim to pay \$75,000 as clearance for anti-drug terrorist fee. Nwokefor finally nailed his victim in the head when she paid him another \$100,000 which was allegedly needed to clear the two boxes of money which had been seized by men of the Customs in Holland.

Daily Sun further gathered that the suspect had been on the wanted list of some of the world's most dreaded security agencies. The criminal branch section of the United States Department of Justice, the US postal service and the Amsterdam Police Department had been on his trail, for his exploits as one of the arrowheads of a Nigerian 419 syndicate that operates from the Dutch city of Amsterdam.

According to a reliable source, Nwokefor left Holland for Nigeria when the heat became unbearable for him. He said: "The US and the Dutch law enforcement agencies notified the EFCC about the case, asking for assistance to secure his arrest. The request received priority attention and on July 27, the fraudster was fished out from his hideout in Lagos."

Nwokefor, who is known by several names, such as Eric Williams, Chika, Lee, Lean, Nago and Nego was based in Amsterdam until January this year when he fled the country for Nigeria after being declared wanted in the Netherlands and USA over advance free fraud cases.

The trial of the suspect had commenced in the US where he was arraigned in absentia before a United States district court, Eastern District of New York, upon indictment for conspiracy, bank fraud, mail fraud and wire fraud. He dropped out of University of Benin in 1998 and travelled to Holland, but was deported in 1999 because of his immigration status.

He was already attracted to the city and could not resist the temptation to try again. To fool the Dutch, he settled for a long winding route in addition to acquiring a false identity. In 2001, he commenced his second journey to Holland. First, he took off to Dubai and from there to Turkey, then, Italy and from Italy he slipped into Amsterdam in 2002. This time he entered Amsterdam as Holger Eweka.

Here is the URL of the article for as long as it is good:

<http://www.sunnewsonline.com/webpages/features/crimewatch/2007/jan/25/crimewatch-25-01-2007-003.htm>

24 JAN 2007

From InformationWeek, an online US magazine:

Official Charged With Embezzling To Pay Nigerian Scammers

Michigan's AG claims a former county treasurer siphoned off \$1.2 million from county coffers, some of which went overseas to fraudsters.

By Gregg Keizer

The former treasurer for Michigan's Alcona County has been arrested and charged with allegedly embezzling \$1.2 million in public funds, some of which he sent to Nigerian-style "419" e-mail scammers.

Thomas Katona, 56, was arraigned in district court last week on 10 felony counts, including embezzlement and forgery, and could face a maximum sentence of 104 years in prison.

According to Michigan Attorney General Mike Cox, Katona directed eight unauthorized wire transfers of county monies, totaling \$186,500, while he was visiting London in late 2006. Six of those transfers were to overseas banks known to have connections with Nigerian fraudsters.

The so-called "419" con, named after the relevant section of the Nigerian penal code because many of the scams originate in that West African country, often starts with an e-mail claiming that the sender has come into a large sum of money. The fraudster needs help in laundering or obtaining the funds, however, and promises the recipient a piece of the action for his or her help, which may include cash payments as evidence of good faith or to speed up the process.

An investigation revealed that Katona had also wired \$72,500 of his own money in June to the same accounts. He was repeatedly warned by bank officials that they suspected he was wiring money to accounts linked to the Nigerian scam. Katona ignored these repeated warnings, said Cox.

A December audit of the Alcona County records showed a shortfall of \$1.23 million, about 30% of the county's \$4 million annual budget. The embezzled monies came out of county investment funds and a revolving tax account, the Alcona County Review, the county's weekly newspaper, reported Wednesday.

"Public officials who violate their oath will be held accountable by my office," Cox said in a statement. "The citizens of Michigan should rest assured that public officials who mishandle public monies will be prosecuted to the fullest extent of the law."

Katona, who served as county treasurer from 1993 until his dismissal in November, remains in custody and faces a preliminary hearing Jan. 31.

Here is the URL of the article for as long as it is good:

<http://www.informationweek.com/industries/showArticle.jhtml?articleID=197000242>

22 JAN 2007

Here is the URL of an amusing Doonesbury cartoon dealing with 419 that is up on the .NeXT Web Security site, enjoy:

<http://www.nextwebsecurity.com/419ScamComic-D1.asp>

15 JAN 2007

The Association of Retired Persons (AARP) Bulletin has a very good article discussing a case of Cashier's Check 419 in its JAN 2007 issue. The article is too long to give here, but here is its URL for as long as it is good:

http://www.aarp.org/bulletin/consumer/when_the_victim_stands_accused.html

8 JAN 2007

Here is News Release NR 2007-2 from the USG Comptroller of the Currency, Administrator of National Banks, which is applicable to Cashier's Check 419 operations, which came out this date:

FOR IMMEDIATE RELEASE:

Contact: Robert M. Garsson
(202) 874-5770

OCC Warns National Banks on Risks Posed by Scams Involving Fraudulent Bank Cashier's Checks

WASHINGTON: The Office of the Comptroller of the Currency issued guidance today warning of the risks posed by scams involving fraudulent bank cashier's checks and describing steps national banks should take to protect themselves and their customers.

A cashier's check, which is issued by a bank and sold to a consumer or other purchaser, represents a direct obligation of the bank.

The guidance was issued in response to a growing incidence of scams involving cashier's checks. In most of these cases, individuals receive a cashier's check and are asked to deposit the check into their account, wait until funds become available and then wire some part of the funds from their account to a third party, often in a foreign country.

One common scam involves an unexpected windfall. The individual is told he has won a foreign lottery or is the beneficiary of someone's estate, and that the proceeds will be sent to him once the taxes or fees are paid. A cashier's check is provided to cover those charges, and the individual is asked to deposit the check and then wire the taxes once the check clears.

In another scam, an individual sells something on the Internet and receives a cashier's check that is greater than the purchase price. The buyer tells the seller to deposit the check and wire the excess once it clears, keeping some amount to compensate for the time and expense involved.

Although funds represented by the cashier's check may be made available to the customer the next business day, and funds availability may be referred to as a check "clearing," funds availability is not a determination that the check is legitimate. Fraudulent checks are very difficult to detect, and it may take several weeks for a fraudulent check to be returned to the customer's bank. When the check is returned, the bank reverses the deposit and withdraws the funds from the customer's account.

Funds availability is governed by the Expedited Funds Availability Act and the Federal Reserve's Regulation CC, which generally require banks to make funds available the next day in the case of a cashier's check. The Uniform Commercial Code addresses the ability of a bank to charge back checks that are returned to it, including fraudulent checks.

Although the funds represented by the check deposited into a customer's account can be removed from the account if the check is fraudulent, wire transfers from the customer's account are an instantaneous and non-reversible transfer of funds.

The OCC recommended that national banks review their procedures to ensure they have addressed the risks posed by fraudulent cashier's checks, and that they take steps to make sure they accurately explain the status of deposited cashier's checks to customers in order to eliminate any confusion.

"Without such information, customers may conclude that a check has cleared solely because the funds are available in the depositor's account," the guidance states.

"Tellers and other relevant personnel should receive appropriate training or other information to accomplish these objectives."

Banks should also consider training to ensure that relevant personnel are aware of the increasing incidence of fraudulent cashier's checks. Tellers could also be trained to examine large dollar checks more closely to identify suspicious cashier's checks, and to ask appropriate questions when customers deposit such items.

Here is the URL of the above News Release NR 2007-2, for as long as it is good:

<http://www.occ.gov/ftp/release/2007-2.htm>

Here is the URL of the Full OCC Bulletin 2007-2 Guidance to National Banks Concerning Schemes Involving Fraudulent Cashier's Checks" on which the above news release NR 200-2 was based, for as long as it is good:

<http://www.occ.treas.gov/ftp/bulletin/2007-2.html>

8 JAN 2007

From the Elsevier Nieuws The Netherlands, a Dutch newspaper, translation by Ultrascan. The story was also covered in other Dutch newspapers:

Nigerian Fraudsters are Still active

Nigerian con men in Amsterdam and Rotterdam continue to be very active in the new year. In the first Five days of this year 4 dutch 419 victims have reported being scammed by Nigerian advance fee scammers. Their average loss was 14.000 Euro.

Nigerian organized fraudsters in The Netherlands have been very successful since 2003, reports Ultrascan which researches this type of fraud. The Con men copy internet sites of Banks. In particular foreign internet users are via emails lured to the fake internet websites of banks like ABN AMRO and SNS Bank, after which they are convinced into transferring money to a bank account. The account is operated by the Nigerian scam ring.

Outside Nigeria itself, The Netherlands are a market leader in harbouring Nigerian scammers, says Frank Engelsman of Ultrascan. Globally the Nigerian gangs are responsible for more than 3 billion Euro damages in 2005. In the Netherlands damages have mounted to 72 million Euro. Engelsman said that on top of that, for last year (2006) there will be a rise reported, but exact numbers were not yet available.

Last year the Amsterdam Police arrested over 70 Nigerians of one scam ring. Since October 1st 2006 the different police departments are working together to attack the

problem. But Engelsman expects little of it. "the police doesn't have enough knowledge in house" he says. Ultrascan pleads for centralized reporting for victims of Nigerian advance fee fraud.

Here is the URL of the original article, in Dutch for as long as it is good:
http://www.elsevier.nl/nieuws/laatste_24_uur/artikel/asp/artnr/133662/

[Go To 419 Coalition Main Page](#)

[Go To 2018 News](#)

[Go To 2017 News](#)

[Go To 2016 News](#)

[Go To 2015 News](#)

[Go To 2014 News](#)

[Go To 2013 News](#)

[Go To 2012 News](#)

[Go To 2011 News](#)

[Go To 2010 News](#)

[Go To 2009 News](#)

[Go To 2008 News](#)

[Go To 2007 News](#)

[Go To 2006 News](#)

[Go To 2005 News](#)

[Go To 2004 News](#)

[Go To 2003 News](#)

[Go To 2002 News](#)

[Go To 2001 News](#)

[Go To 2000 News](#)

[Go To 1999 News](#)

[Go To 1998 News](#)

[Go To 1997 News](#)

[Go To 1996 News](#)