RED ALERT ON SCAM

Introduction

Advance Fee Fraud and its variants are confidence scams. Typically, such scams involve a promise of a huge slice of a large sum for which the fraudster requires some up-front payments in bits and pieces. Overtime, such payments add up to a huge heist.

In recent years, Nigeria and indeed West Africa have been tagged as the home of Advance Fee Fraud. But far from it, the crime is indeed an international organised crime that is not limited to a single national or regional boundary. Indeed it is said to have developed in the late 19th century from the ashes of what was known as Spanish prisoner scam, where businessmen were contacted by an individual allegedly trying to smuggle someone connected to a wealthy family out of prison in Spain. From the Iberia Peninsula, the scam has grown in sophistication and spread to the extent that there is hardly any nation today that can be said to be completely immune from the scourge. According to 2006 statistics, 61 percent of internet criminals were traced to locations in the United States, while 16 percent were traced to the United Kingdom and 6 percent to locations in Nigeria.

What this simply means is that Advance Fee Fraud has metamorphosed into a multi-national organized crime that does not respect national or regional borders. It is therefore not surprising that the US, UK, the Netherlands, Russia, Malaysia, South Africa, Pakistan, Nigeria, Spain, Togo, Benin, Ghana, India and Kazakhstan are listed among nations with high incidence of the scam.

Many Nigerians are themselves victims of this criminal enterprise, losing unreported hundreds of thousands of naira yearly to confidence tricksters. The truth is that fraudsters do not really care about nationality; they strike wherever and whenever they see even the slimmest chance to swindle others. On the internet, through the telephone and even physical interaction, the deadly predators are perpetually stalking the rest of us.

We have distilled, in this small book, many of the avenues through which fraudsters can scam you. It is our expectation that this effort will awaken your consciousness to the many ways scammers could target you as well as how you can guard against becoming the next victim of '419'.

It is not unusual to hear some people boast that they could never be victims of scam on account of their education or status! They may be right, but available records show fraudsters make no discriminations as to the social status or

level of education of those they set their sights on; the most educated, most exposed individuals as well as the most ignorant members of the society have been victim at one time or the other. The young as well as the aged have been successfully scammed.

In the last few years EFCC has arrested and prosecuted hundreds of fraudsters and sent them to jail. But jail has proven not to be enough deterrent, judging by the increasing incidences of 419. Ultimately, prevention is the most effective way of tackling the malaise.

If you want to be insulated from scam, the inoculation you need is adequate information. Arming yourself with relevant information on the different types of scams and the modus operandi of their perpetrators, primes your senses to trigger the alarm when things are not as they should be. There is a lot of information to be found in EFCC publications, on our radio and television programmes, The Eagle, as well as on our website, efccnigeria.org and other social media platforms- Facebook, Twitter, Instagram and YouTube.

The following are some of the common types of scams. (The list is by no means exhaustive).

TABLE OF CONTENTS

1. Banking and Online Account Scams

Many individuals have been defrauded by being careless with their personal banking details. A response to what looks like a harmless request to update account information has led many people into financial misery.

How It Works:

E-Commerce/card frauds are usually perpetrated through phishing and spoofing. What these entail is that the scammers send e-mails with fake letter heads and logo of banks, pension fund managers and similar organisations, to unsuspecting members of the public, seeking vital personal identification information. Such information may include user login details, pin and password. Usually they add the clause that the information is needed for the updating of your account and that if it is not made available within a stipulated period, your account may be closed.

Sometimes they direct you to a look-a-like website where you are expected to upload all information about yourself and your bank account. Once you respond to the mail with the right answers to the information they seek, the scammers quickly set to work by making withdrawals from your bank account. Variants include pet sales, car sales, vacation rentals scam, etc.

WHAT TO DO:

ASK YOURSELF: Why will my bank ask me to update my account?

FIND OUT: Did the request to update your account actually emanate from your bank? Visit or contact your bank to be sure.

REMEMBER: Banks and other financial institutions never ask for your personal Identification details (they already have all the information they need about you). And, they always advice that on no account should anyone disclose this information to third parties.

SAFEGUARDS: Do not give out information about yourself to anybody you don't know. Never respond to any mail you are unsure of its source. Visit or contact your bank to confirm any request for information.

2. Ponzi Schemes/Wonder Banks

This is a fraudulent investment scheme promising high rates of return with little risk to investors. The scheme generates returns for older investors from the investment of new entrants. This scam thrives as earlier subscribers who are paid huge returns spread the words and get more people

to join the bandwagon. The schemes usually collapse when new investors are no longer forthcoming.

It typically starts with one person - the initial recruiter - who is at the apex of the pyramid. This person recruits a second who is required to "invest" a certain amount, which is paid to the initial recruit. In order to make his or her money, the new recruit must get more people under him or her, each of whom will also have to invest. If the recruit gets 10 more people to invest, he or she will make a profit with just a small investment. These schemes usually collapse on themselves when the new investments cease.

In the case of wonder banks, the victim invests in a scheme and is promised mouth-watering returns within a short period of time beyond the range of interests on fixed deposits payable by commercial banks. The scheme thereafter collapses and the owners disappear into thin air, while depositors lick their wounds

What to Do:

ASK YOURSELF: Where does the company get the money to pay investors the fantastic returns on investment within a short time?

FIND OUT: With the relevant government regulatory agencies to see if it is a registered investment company.

REMEMBER: All companies providing investments services to potential and existing clients usually detail how and where the money will be invested and also the profile of returns on investment.

SAFEGUARDS: Do not invest your money in any business that has no clear prospectus on how it operates. Be wary of investments with unusually high rate of returns in the short term.

3. Romance & Dating Scams

The fairy tales of people meeting on the internet and starting a relationship that eventually end with the couple getting married have not ceased to fascinate many. Those who are truly emotionally drained and are in need of partners have embraced the many dating sites on the Internet to fish for partners. Such sites have also unwittingly become the hunting ground for fraudsters.

How It Works:

Romance scam is perhaps the most common form of cybercrime. The scammers play on the emotions of those who are genuinely interested in love to defraud them.

What the fraudsters do is to use existing free dating websites to deceive unwary love seeking individuals

The stories that love scam artists spin to bait and extort their victims are many. Mostly, they are stories that appeal to the emotions of the unsuspecting victim. For instance, they could get somebody to call their would-be victim with the information that his/her lover had been involved in a terrible accident and desperately needs money to pay medical bills. Usually photographs of an accident scene are mailed to the unsuspecting lover.

They can also request for help to transfer some huge money, necessitating the request for the victim's banking details. Such requests are made after a reasonable relationship had been established. Once the information is released, it is used to fleece the victim.

What to Do:

ASK YOURSELF: Will a person you have never met be professing genuine love to you after only a few exchanges of e-mails?

FIND OUT: If the person you are communicating with is the person whom he/she claims to be.

REMEMBER: The emotional cost of romance scam could be tragic and devastating.

SAFEGUARDS: Be very suspicious of stories you are told by supposed lovers in an Internet love affair. It pays not to be too emotional and to cross check every information.

Above all, never send money or disclose your banking details to any one you hardly know or trust. People should be wary of those they meet on dating sites. Demand for a live video conversation/chat.

4. Employment Scams

Scammers have cashed in on the unemployment situation in the country and the preference of many unemployed people for certain sectors of the economy to dupe unsuspecting job seekers.

HOW IT WORKS:

Employment scams can take the form of job advertisement in newspapers and online platforms. Those who apply are asked to pay a token to have their applications processed. There are limitless excuses for the request for fees from job seekers. However, once the fees are paid, the scammers disappear. Where they are not offering non-existent jobs, they could ask job seekers to pay registration fees for phony seminars to improve their job skills and brighten their employment prospects.

Such scams can also be perpetrated through offers of mouthwatering positions by fraudsters on the internet. Though different categories of staff are said to be needed in the advertisements, it is mostly, top management positions in the oil, gas and telecommunications sectors

that are emphasized. Commonly, the targets are expatriates. Once a potential victim applies, the scammers ask for their personal details and other relevant information. They would then request visa fees and sundry charges to process documents, resident permits, and verification of documents by some bogus government agencies.

What to Do:

ASK YOURSELF: Is this advertisement real?

FIND OUT: About the supposed organization or positions advertised

REMEMBER: Any job advertisement that promises outlandish salaries and perks is suspicious. No credible employer demands pre-employment payments for whatever reason from prospective employees.

SAFEGUARDS: Remember, no credible employer will ask you for money to process your employment. Disregard any offer once request for money is made. Seek advice from relevant authorities.

5. Identity Theft/ Phishing Scams

Identity theft is the act of a criminal, wrongfully obtaining information about someone else and using such information to commit aid or abet any unlawful activity for economic

gain. In this type of scam, one's identity and/or contact information are compromised and used by criminals for financial gain.

How It Works:

Fraudsters using phishing, key loggers, malware, social engineering sim card cloning methods obtains or take over victim's identity, email or telephone numbers which are later used to contact known acquaintances. The impostor uses the victim's contact information to make monetary demands usually through bank transfers from his/her personal and/or business acquaintances. The impostor always avoids communication with the potential victim at this period.

What to Do:

ASK YOURSELF: Has my acquaintance made such a request before?

REMEMBER: Always confirm sudden distress messages before any financial assistance is rendered

SAFEGUARDS: Verify the caller's claim before you take any step to help. If the solicitation is by email, ensure you authenticate through a phone call. Get independent confirmation from a third party when sudden distress calls or messages are received. Avoid using the same password across all your online platforms. Change your passwords at

regular intervals. Always log out of online platforms after use of any electronic device.

6. Contract Scams / Funds Transfer

When you have not executed any contract but receive messages from unknown persons seeking your favour to remit payments for jobs executed into your account for a cut of the money, you are about to be scammed.

How It Works:

A prospective victim is told that a certain government agency or committee is processing the payment of a contract purportedly executed in the past and that the victim should provide his bank details so that money can be transferred to him/her. A response automatically engenders unending demands for advance payments until the victim comes to the realization that he/she has fallen into the hands of scammers. This type of scam is a classic advance fee fraud in which several fake documents are used in furtherance of the scam

A variant of this scam involve solicitations for the use of your bank details to transfer stolen funds from a country, usually an African country. The requests often come from fraudsters claiming to be relations of ranking government officials or children of a dictator ousted from power.

What to Do:

ASK YOURSELF: What qualifies you to get a cut of a contract you knew nothing about and from a person you have never met?

REMEMBER: No genuine contract is awarded on the internet or via the phone

SAFEGUARDS: Never be part of any transaction that seems dubious or which you might not be comfortable discussing with family, friends and associates. Any transaction cloaked in secrecy is most likely an expressway to financial perdition.

7. Inheritance Scams

Everyone loves the sweet aroma of inheritance but if your parents and family members have not bequeathed any wealth to you, you might endanger your financial health if you suddenly believe such inheritance can come from total strangers.

How It Works:

A letter suddenly appears in your mail box, from somebody who claims to know you or who got your contact from a friend, asking for your assistance to transfer an inheritance left by a dead relative or friend. Such letters are typically made out to be from a lawyer or a bank representing the interest of the deceased.

In the process of trying to claim the inheritance, you are asked for documents and personal banking details. Then you are asked to pay fees and taxes and your identity could also be stolen in the process.

This scam is perpetrated in different ways. A scammer may introduce himself or herself as a top manager of a bank and tell you there is a dormant account in the bank with money which belongs to one dead wealthy person, which relatives of the deceased are unaware. They tell you they need your account details to move the 'trapped funds.' Once you respond to the request, they will continue to ask you for more money.

What to Do:

ASK YOURSELF: What informed your choice as the one who could help secure the inheritance.

REMEMBER: Issues of inheritance are dealt with at the court of law and not through the internet.

SAFEGUARDS: Take such stories with a pinch of salt. Be conscious of the fact that nobody will want to involve a total stranger in sharing his inheritance. Never take the request for assistance on the face value, investigate.

8. Charity Scams

Scammers play on people's benevolence mostly by spinning stories calling for voluntary donations in furtherance of such events.

How It Works:

The scammers collect money by pretending to be genuine charities. Usually, fraudsters seek to cash in on any natural disaster that is in the news by posting heart-rending stories or photographs on the internet. They request monetary assistance to help victims of such disaster or crisis. Such monetary assistance, they claim, will help pay medical bills, provide feeding and a host of other charitable services.

Again, there are those who come under the guise of religion by appealing to your conscience to give towards the building a church, mosque or an orphanage.

There are also those who solicit money or contributions to meet the demands of a particular situation. Sometimes they use pictures of or disabled persons who need urgent medical care.

Some use stories that they run orphanages and send pictures showing them with orphans.

All these are done to appeal to the conscience of potential victims and make them part with hard earned money.

What to Do:

ASK YOURSELF: Who is behind this charity? Is the cause genuine?

FIND OUT: If those you are paying to are indeed affiliated and/or representing the cause.

REMEMBER: Charities are not anonymous. They are registered legal entities with real trustees.

SAFEGUARDS: Carry out your own investigation and ensure that you are dealing with the genuine operators of a charity.

9. Juju Scams

In some parts of the world, especially African societies, it is believed that spirits and deities possess supernatural powers which they deploy either for good or ill. One of such beliefs which have strangely not been mitigated by modernity is the power of such forces to confer wealth and provide spiritual solutions to diverse problems. Fraudsters have cashed in on this notion which is still popular in Africa and the Caribbean to swindle unsuspecting victims

How It Works:

This scam comes in various guises but mostly involves claims of invocation of the powers of deities and other supposed spiritual forces touted to have powers to confer benefits on

victims. Frequently, victims are taken to shrines in remote villages and towns where they are propositioned by a priest (usually one of the con artists) to receive instructions from a supposed spiritual force on what to do to solve the problems. And to foreclose detection, victims are warned never to discuss such encounters with anyone. Failure to heed such warnings, they are made to believe, carries consequences, including death.

The instructions from the spiritual forces always end with request for money for some cleansing exercise or to buy one item or the other. Pliable victims continue to pay until they are milked dry.

What to Do:

ASK YOURSELF: Do they have the capacity to solve my problems?

REMEMBER: There is no shrine or deity that has the ability to make you rich or solve your problems.

SAFEGUARDS: Never accompany anybody to shrine or spiritualist for purposes of receiving a formula that will make you rich. Above all, whenever you are called to come to a shrine to receive some wealth potion or get your problems solved, know that you are being positioned to be scammed or fleeced.

10. Lottery Scams

With the global economic downturn, people have come to embrace lottery wins as a quick avenue to make money. This is not lost on fraudsters who have cashed in on this trend to dupe several people. A simple text message alerting some people that they have won one lottery or the other (even when they did not participate in the first place) have seen them emptying their accounts to pay fees and taxes to claim non-existent prizes.

How It Works:

Scammers usually send e-mail, make phone calls and send text messages informing you that you have won a prize even when you did not enter any contest. They entice people with some mouth-watering prizes. But there is always a caveat: you are told to make payments before you finally collect the prize. This scam targets mass victims.

What to Do:

ASK YOURSELF: Did I participate in any lottery? If the answer is in the negative, then my winning is a scam.

FIND OUT: If there is any such lottery in operation at that time and how people emerge winners.

REMEMBER: You cannot win a competition you have not entered.

SAFEGUARDS: No lottery company will ask for winners to make advance payment to collect the lottery prize. Always delete unsolicited bogus mails and ignore dubious text messages and telephone calls.

11. Crude Oil/ Mineral Resources Sales Scams

The extractive Industry is highly lucrative. The allure of making quick investment breakthrough in the sector has sent many to financial ruin.

How It Works:

The fraudster makes contact, offering to sell petroleum products, precious stones, etc, to potential victims at a ridiculously discounted rate, far below world market price. They convince the prospective victims to invest in the business. The scammers who are conversant with the workings and technical details of the industry provide samples and other documentation to convince the victims. They also create websites. Once convinced, payments are demanded for phantom products.

What to Do:

ASK YOURSELF: Are minerals resources sold on the internet?

FIND OUT: More about the transaction from relevant agencies and other traders.

REMEMBER: Crude oil and mineral resources are sold on the international commodities exchange by reputable traders and not opaque businessmen.

SAFEGUARDS: Never close an oil deal without carrying out proper due diligence check on the companies and individuals involved.

12. Wash-Wash (Money) Scams

In this day and age some people still believe that it is possible to sit somewhere, either in their homes or at a shrine and be printing fresh high denomination currency notes, whether naira or foreign currencies. They fail to reason that no one would let people into the secret of money printing if they knew it.

How It Works:

The tricks employed by fraudsters who dominate this trade are many. A fantastic proposition could come in the mode of an offer of a large consignment of dollars that needs to be 'washed' to become spendable because it is currently marked. A typical scenario could be that a few genuine dollars are neatly and carefully arranged on top of fancy trunk boxes of large quantity of fake or blank papers which appear as real dollars in a controlled environment.

A few of the genuine dollars which are marked are 'washed' and may be spent in the presence of the

potential victims to further convince him that the deal is real. Other members of the syndicate will try to convince the potential victim that he should get more money for them to clean the other 'dollars' and that he would be highly rewarded.

The snag, however, is that the chemical needed to ‘wash’ the ‘dollars’ is very expensive and difficult to come by. Contact is made by the scammers to other members of the syndicate in the presence of the would-be victim who tells them where they can get the chemical and how much is needed to purchase it. Thereafter, much persuasion is made to ensure that the would-be victim brings the money to clean up the other large consignment of ‘dollars’. And he is told not to share the information with anyone in order not to be schemed out of the deal.

At other times would-be victims are taken to shrines in remote villages where they are made to listen to supposed spirits asking them to bring money for sacrifices to make them rich.

The truth only becomes obvious to the thoroughly fooled victims once they part with their hard earned money.

What to Do:

ASK YOURSELF: If it were possible to produce currencies simply by applying chemicals to papers, would these people be willing to involve you?

REMEMBER: Genuine currencies can only be printed and circulated by government. Report to the nearest police station or EFCC office.

SAFEGUARDS: Monies cannot be produced by the application or washing with mere chemicals.

13. Scholarship Scams

Many families yearn for assistance to give their wards a decent education. Fraudsters have also cashed in on this to defraud people.

There are many websites on the internet that are offering scholarship for persons that are eager to study abroad. But if you do apply and you are told that you need to pay some money to process your application it is most likely a scam. So, avoid making payment either on-line or through the bank for any offer of scholarship. No genuine scholarship offer is offered for a fee.

What to Do:

ASK YOURSELF: Do I need to pay fees and charges to get a scholarship?

FIND OUT: The status of the organisation or educational institution.

REMEMBER: Scholarship awards involve competitive processes for deserving candidates.

SAFEGUARDS: No genuine offer of scholarship would demand any payment as scholarship is free. Do not make any payment when contacted. When in doubt, visit the home embassy, office or website of the awarding organisation/educational institution to ascertain the veracity of the offer.

14. Auction / Product Scams

An attractive product advertisement, with generous discount offer could be bait to financial misery

How It Works:

Most victims of this scam are foreigners. What scammers usually do is to advertise a product or goods for sale on the internet at heavily discounted prices to attract buyers. Once a buyer indicates interest in the product, they start to extort money by coming up with all kinds of bogus charges for such things as demurrage, clearance, certification and a host of others.

For example, a scammer EFCC eventually sent to jail, once advertised on the Internet that he had rail scrap for sale.

Unfortunately a genuine Turkish businessman saw the advertisement and indicated interest to buy. The scammer persuaded the Turk to come to Nigeria and view the goods. Once he came, the businessman was taken to the Nigeria Railway Corporation compound, where he saw tons of rail scrap, which further convinced the innocent businessman as to the authenticity of the deal. Thereafter he was made to part with $80,000 which he was told was the cost of the goods. All he took back with him to Turkey was a promise that the rail scrap would be shipped to him in a few weeks. However, once he returned back to base, the scammers started making further request for money which they claimed they needed to settle government officials to fast track the shipment of the goods.

If you are also somebody that sells products online, scammers can also target you by offering payment in cheques that far exceeds the value of your products. You are told the excess payment was in error and then requested to make a refund via money transfer. Most people, who pay such refund, discover later that the cheque is a counterfeit. In this instance, the victim loses both ways: the product and the transferred money.

What to Do:

ASK YOURSELF: How genuine is the deal? Verify from relevant authorities

FIND OUT: Any proposition that sounds too good to be real should be treated with circumspection.

REMEMBER: Any deal that looks too good to be true is suspect.

SAFEGUARDS: Do not be in a hurry to make payments. Do due diligence before committing your funds to any transaction.

15. Emergency Scams

Not every call to save the life of a relative or an acquaintance in distress is genuine. This type of scam usually targets Nigerians and other Africans.

How It Works:

Another form of emotion scam come in the likes of solicitation for payments to save a relative in distress. It usually starts with a phone call informing a person that his/her child or relative has been involved in an accident or some sudden life threatening emergency. The caller could simply say "your child or brother who is schooling in the United States or Britain has been involved in an accident and he is in a coma'.

To further convince the victim, the person calling who pretends to be a doctor or nurse would inform the would-be victim that a search through 'injured' or 'sick' person's phone indicated the victim as a parent or relative. Yet another member of the syndicate may call to claim that he or she is a friend to the injured person and that before the accident, they had discussed some of his family issues. Usually the potential victim may be warned not to inform other members of the family so as not to trigger anxiety in the family. The warning is then followed with demands for the remittance of some money to save the life of the supposed accident victim. They will usually direct their victim to transfer money to them. Usually it is after the victim would have transferred the money that he would realise that he had been duped.

What to Do:

ASK YOURSELF: Do I have any relative that could be in such emergency situation?

REMEMBER: To call your relative to verify the claim.

SAFEGUARDS: Do not answer leading questions about any relatives from strangers. Verify the caller's claim before you take any step to help. Do not part with your money to somebody you don't know. Get independent confirmation from a third party when sudden distress calls or messages are received.

16. Immigration / Visa Scams

The search for greener pastures abroad have led many into taking desperate steps to realise their ambitions to travel overseas, especially to Europe and North America. Fraudsters have capitalized on this to dupe many would-be immigrants.

How It Works:

The scammers claim to have connections at embassies or with persons who can help secure entry visa and other travelling documents for those seeking to emigrate. They demand various fees and charges to procure vital travel documents. While the scheme lasts, they keep telling stories to support the unending demands for more money. Eventually, if they do not disappear with the victim's travel documents, they may issue a fake visa to the unsuspecting victim who certainly would be arrested at exit or entry ports.

What to Do:

ASK YOURSELF: Why pay money for visa and other documents to an agent when you can deal directly with the embassy?

REMEMBER: Biometrics has made it impossible for anybody without genuine travel documents to procure a visa.

SAFEGUARDS: Go to the embassy of the country you intend to visit, to process your documents yourself. Most countries issue visas directly through their embassies and not through third parties/agents. Check the official website of the intended country of visit for guidelines. Pay visa fees into designated embassy account.

17. Local Purchase Order Scams

Orders to supply goods have turned some people to millionaires just as they have sent many to financial ruin.

How It Works:

The prospective victim is usually given a Local Purchase Order, LPO, to make supplies in the name of a company. The scammers make the profit margins so attractive and irresistible to the victim. The victim is given a fake LPO and instructed to make the supplies to a designated warehouse or office. Once the goods are supplied, the victim would be told to call back the following day or the week after to get payment, which is never forthcoming. Once the scammers succeed in buying time, they disappear without a trace. The victim suddenly finds out that he has been conned.

What to Do:

ASK YOURSELF: Is the margin of the LPO reasonable?

REMEMBER: Always take additional steps to verify the genuineness of LPO and the true identity of the persons you are dealing with.

SAFEGUARDS: Don't accept every LPO especially when it comes too easily. Be wary of fantastic profit margins on LPO transactions. Confirm and re-confirm that the LPO is genuine and that the company issuing it is reputable.