

Global Security

Advance Fee Fraud

The 'Set Up' Proposal

Advance Fee Fraud, or '4-1-9' Fraud as it is more commonly known, is perpetrated by sending bogus business proposals by fax, letter or, most recently, email, offering rich rewards for the use of existing accounts to transfer money out of Nigeria. This type of fraud has been around for many years, and has been targeted at small businesses, wealthy individuals and large Corporations, preying upon the desire to make 'easy money'. It would surprise most people to know how many have fallen for the ploy, and consequently lost large amounts of money.

Those carrying out the frauds obtain the names of potential victims from a variety of sources, including trade journals, professional and company telephone directories, newspapers and commercial libraries. Every year millions of 'letters' are sent worldwide and official estimates show that 10% are answered, i.e. show initial interest, and 1% of recipients actually get involved, in some cases losing as much as \$1 million in a single fraud.

The proposal takes many forms, but in most cases will hint that huge amounts of money have been obtained through illegal business dealing, and that it is necessary to have a 'clean' account to transfer the money out of Nigeria. The offer will request a telephone/fax number; the name, address and telephone number of the bank holding the account, together with the account number and sort code. There is also a promise of 20% of the funds for the use of the account. It is common for the proposal to be on fake government documents, purporting to be from the Presidency in the Federal Capital Territory (FCT) Abuja, Ministry of Defense, Nigerian National Petroleum Company (NNPC) or the Nigerian Federal Ministry of Works (NFMW); although it should be emphasized the list is not exhaustive.

The Fraud

Once interest is shown, the victim is faxed a mass of 'official documents' to legitimize the deal, before being asked for 'up front' payments to cover unpaid taxes, currency exchanges, gratuities for corrupt officials or other 'unforeseen' expenses. When the promised transfer funds fail to appear in the account, and the victim complains, he will be told to travel to another country and contact a mobile telephone number. Over a number of meetings the fraudsters will then attempt to extract more money using other 'scam' methods.

Alternatively, the given account will be drained of funds by the use of a variety of forged financial instruments, such as Letters of Credit, Certificates of Deposit, Bills of Exchange, and the like.

Many victims refuse to report their losses to the authorities, either through personal embarrassment, or the fear of being implicated in a fraud against the Nigerian Government. It should be noted that in some countries the law enforcement agencies will prosecute victims for such offences. The Nigerian Police Force has set up a dedicated cell to investigate the crimes, but the reluctance of victims to press charges has hampered their investigations.

To further the Nigerian Government determination to reduce the amount of 4-1-9 fraud, an amended decree now empowers the State High Courts to try offenders. Additionally, a high profile campaign to publicize the '4-1-9' frauds has also been undertaken.

In The United States, the U.S. Secret Service has established "Operation 4-1-9", an effort designed to target the Nigerian Advance Fee Fraud on an international basis.

The United States Postal Inspection Service is considering opening a satellite office within the U S Consulate in Lagos , Nigeria , to liaise with government law enforcement officials.

Latest Variations

Two recent variations of this scheme, have surfaced in the United States , Canada and Australia . In the first instance, someone posing as a wedding planner, representing an ExxonMobil executive whose child is about to be married, contacts a limousine company to rent cars for the event. The planner negotiates the rate either by phone or e-mail and sends a deposit (usually more than the agreed amount) via certified check or money order. Shortly after the funds have been received and deposited by the limousine company, the planner calls to report a tragic occurrence, such as the death of the executive, which requires a cancellation of the wedding. A refund is requested and if the limousine company complies before allowing a suitable amount of time for the check or money order to properly clear, they are usually shocked to learn that the financial instrument/s was bogus and that their accounts have been debited for the loss.

In the second instance, someone poses as a representative of ExxonMobil contacts hotels or resorts to reserve space for a business meeting. The deposit, in check or money order form, arrives in the mail in an envelope with an ExxonMobil logo. The event is suddenly cancelled and a refund is requested. As in the above scenario, if the refund is made before the check or money order clears (which it won't), the business suffers a loss once the deposits bounce.

Other variations of this scheme have been reported that utilizes the ExxonMobil name (or variations thereof) in e-mail solicitations involving employment or business opportunities within ExxonMobil. These e-mails are not typically sent to employees or business partners on the company's Lotus Notes system but rather have been received by annuitants and contractors on private e-mail providers such as *Yahoo.com* or *excite.com*.. The fraudsters utilize otherwise legitimate websites such as *Monster.com* or *SEEK.com*, to obtain information about prospective applicants and try to lure unsuspecting people into the trap.

The positions offered are outside of the applicant's country of residence and generally in developing countries such as Nigeria or Angola . After contact is established, there are a series of "reimbursable fees" that need to be paid in advance, for such things as visas, insurance, in country licensing, etc., before employment can actually begin. The applicant may be invited to an actual ExxonMobil facility such as St. Catherine's in London , for interviews and processing. Of course, this only occurs after advanced fees have been paid.

The bogus e-mail solicitations utilize variations of the ExxonMobil name in their headings. The bogus e-mail attachments have ExxonMobil (or affiliate) letterheads along with a host of typical approval stamps and certifications.

Bogus business opportunities utilize actual ExxonMobil graphics that have been cut and pasted from the company's legitimate website. The offering is typically from a supposed ExxonMobil manager outside of the US with a business opportunity in another part of the world.

Lessons Learned

ExxonMobil has received many of these proposals at offices throughout the world, but there are no recorded cases of Company employees becoming victims of such fraud.

Beware of giving business or personal details, including financial, over the telephone, particularly if you are unable to positively identify the caller, and ensure any documents containing such data are shredded, rather than just thrown away.

The receipt of any unsolicited business proposal, other than through regular channels, should always be treated with suspicion, particularly if incentives are offered. It should be reported to Line Managers immediately, with the original letter, fax or copy email being preserved for handing to the local law enforcement agency.

What You Should Do

Do Not respond to the fraudsters, even if your intent is to inform them that you are aware of their misrepresentations. All you will succeed in doing will be to provide them with a legitimate point of contact (you) and you may find yourself besieged by similar offerings or having your name used in future offers.

The jurisdiction for handling a 4-1-9 case resides with the location where the proposal is received, or from where it is sent. As each country may have different methods and law enforcement agencies dealing with them, it is not possible to issue 'blanket' advice regarding actions. However your Security contact should be aware of the local procedures for passing the information to the relevant authority.

Proposals that are received should be dealt with locally or regionally by the appropriate Security Business Center.

However, if there is any suggestion of:

1. Impact on the business interests of ExxonMobil,
2. An employee becoming a victim,
3. A nexus between the proposal and any Company personnel, information or asset.

The correspondence should be forwarded to Tony Marley, Security Advisor for Nigeria at 234 1 262 1640 Ext. 1036, with a brief explanation as to the circumstances and any action taken, for due investigation. Tony Marley may be contacted by email at anthony.d.marley@exxonmobil.com.

In The United States, the U.S. Secret Service has asked that if you have been victimized by one of these schemes, the appropriate documentation be forwarded to them. In response to this request, please forward any solicitations received by mail, to Hank Sarno, c/o ExxonMobil, 1400 Old Country Road, Suite 203 , Westbury , New York , 11590. Bogus or suspected e-mails should be sent to hank.c.sarno@exxonmobil.com.
