The voice of banking & financial services

Common fraud schemes

Information for bank customers

This leaflet provides an outline for bank customers of some of the most common types of financial fraud schemes, along with advice on practical steps customers can take to help them avoid falling victim to fraudsters.

1. Advance fee schemes

An advance fee scheme occurs when the victim pays money to someone in anticipation of receiving something of greater value, such as a loan, contract, investment, or gift, and then receives little or nothing in return. They may involve the sale of products or services, the offering of investments, lottery winnings, “found money”, or many other “opportunities”.

Clever con artists will offer to find financing arrangements for their clients who pay a ‘finder's fee’ in advance. They require clients to sign contracts in which they agree to pay the fee when they are introduced to the financing source. Victims often learn that they are ineligible for financing only after they have paid the ‘finder’. Such agreements may be legal unless it can be shown that the ‘finder’ had no intention or ability to provide financing.

Tips to avoid advance fee schemes

- If the offer of an ‘opportunity’ appears too good to be true, it probably is.
- Know who you are dealing with. Learn more about the person or company.
- Make sure you fully understand any business agreement you enter into. If the terms are complex, have them reviewed by a competent attorney.
- Be wary of businesses that operate out of post office boxes or mail drops and do not have a street address, or of people who do not have a direct phone line.
- Be wary of deals that require you to sign nondisclosure or noncircumvention agreements designed to prevent you from independently verifying the bona fides of the people with whom you intend to do business.

The voice of banking & financial services

2. Lottery scams

Lotto frauds are widespread in the UK with promises of huge winnings arriving via unsolicited e-mail or letters. Invariably the communication will purport to come from an overseas lottery and claim that the recipient has been allocated winning numbers.

The recipient will be asked to contact the organisers and invited to send money in to assist in the administration for the release of the winnings.

In the case of e-mail anyone can be a victim; these spam e-mails are sent en-bloc. With letters, the criminals can be more specific and in many cases they will target the elderly. False certificates of winnings will be sent. The victim may respond and after sending a fee to the fraudsters may have telephone contact seeking further money.

Case Scenario
An elderly couple, both in their nineties, went into their bank and wished to draw out more than £20,000. When asked why, they told the bank they had won money in an overseas lottery and were paying some fees to release the money. The bank advised them that this was a fraud and tried to deter them from drawing out the money.

The couple demanded that unless the bank allowed them to do so, they would close their account and take their business elsewhere. The bank contacted the fraud squad and a manager from the bank together with a detective from the fraud squad visited the couple and convinced them that this was a scam, preventing the loss of their life savings.

3. Share sale (or 'boiler room') fraud

Sale share fraud, also known as boiler room fraud, occurs when someone you don't know rings you up and tries to sell you shares. Boiler room firms use convincing sales tactics to persuade you to buy shares which are of little or no value.

You will almost certainly lose all the money you spend.

The vast majority of share sale fraud victims are experienced investors, with 41 per cent of victims saying they had been investing for over 11 years – it is not just the novice investor who can be duped in this way. The Financial Services Authority estimates between £200 and £500 million is defrauded from victims in the UK every year.

The voice of banking & financial services

The first time you hear from a share sale fraudster could be by post or email. They may have written to you offering a free research report into a company in which you hold shares, or a free gift or a discount on their dealing charges. You will then receive a phone call from a well trained, highly professional sounding salesman. They can be very persistent, never taking 'no' for an answer. They often use a script to help them answer your questions or ward off your objections. They phone their victims every day until they finally make a sale, or until you hang up.

They will often claim to be from legitimate firms, or firms which sound legitimate and have professional looking websites. You may be told that you have already entered into a contract to buy the shares and are under an obligation to pay. This is not the case as such contracts are unenforceable under UK law.

If you deal with a share sale fraudster or boiler room you will have no rights to complain or claim compensation in the UK, as these frauds are based overseas, despite what the caller may say. They are not authorised by the FSA to do business in the UK.

Generally it's against the law to 'cold call' a person to try to sell shares or other investments. So if you haven't invited the call just hang up!

Tips to avoid share sale fraud:

- Always ensure the firm is on the FSA Register and is allowed to give financial advice before handing over your money.
- Double check the caller is from the firm they say they are – ask for their name and telephone number and say you will call them back. Check their identity by calling the firm using the contact number listed on the FSA Register.
- Check the FSA's list of known authorised overseas firms at www.fsa.gov.uk/pages/doing/regulated/law/alerts/overseas.shtml
- If you have any doubts call the FSA Consumer Helpline with details, or complete the 'Unauthorised firms reporting form'.

The voice of banking & financial services

4. Telemarketing fraud

When you send money to people you do not know or give personal or financial information to unknown callers, you increase your risk of becoming a victim of telemarketing fraud. Tell-tale “lines” a caller may give the victim include: “You must act now or the offer won't be good"; "You've won a free gift, holiday, or prize – but you have to pay for ‘postage and handling’ or other charges”; "You must send money, give a credit card or bank account number, or a cheque."

Tips to avoid telemarketing fraud

- Never send money or give out personal information to unfamiliar firms or people.
- Get the salesperson's name, business address, phone number and business licence numbers (Office of Fair Trading Consumer Credit Licence number or Financial Services Authority registration). Check the accuracy of these items.
- Ask for written material about any offer or charity. If you get brochures about investments, ask someone whose financial advice you trust to review them.
- Before you give to a charity or make an investment, find out how much is paid in commission.
- Before you send money, ask yourself: "What guarantee do I have that this individual will use my money in the manner we agreed upon?"
- Do not pay in advance for services; pay only after they are delivered.
- Avoid snap decisions and never respond to an offer you don't understand. Talk over big investments with a trusted friend, family member or financial advisor.

5. West African letter / email fraud

West African letter frauds, also known as 419 frauds, involve asking you to help with transferring money out of another country - such as Iraq, South Africa or somewhere in West Africa - in return for a percentage of the money you helped to transfer.

There is no money to transfer.

Generally, you receive an email, letter, fax or phone call from a fraudster claiming to be someone in a position of authority. The fraudster says they have access to a substantial amount of money and explains where this money is supposed to have come from. They say they want to move the money out of the country, then give a reason why they can't transfer it themselves, such as they can't open an overseas bank account. The fraudsters will also explain why you have been chosen to take part in this venture, perhaps saying a mutual acquaintance has recommended you for the role.

They ask your permission to pay the money into your account before they transfer it onwards after deducting your reward. The fraudsters may even ask you to open a new bank account to transfer the money. They will also emphasise the need for secrecy, warning you not to tell anyone else about the deal while hurrying you into a hasty decision by stressing the need for urgent action. To add an element of legitimacy to the fraud, the fraudsters may arrange to meet you, normally outside the UK. The fraudsters may also ask you for details of your bank account so that they can transfer your reward. They will use this information to try and empty your account.

If you respond to the fraudsters' request, they will ask you to pay various fees that are supposed to release the money. For example: legal fees, transaction fees or taxes. When you pay the first fee, the fraudsters will keep coming back with further requests for additional fees, explaining that each one has cropped up as a last-minute obstacle to releasing the money.

Tips to avoid West African letter / email fraud

- Be sceptical of someone you have never met who saying they trust you with a large sum of money.
- Governments and large corporations do not transfer money through another person's bank account. Any suggestion that they do so is a reliable indication that you have been approached by fraudsters.
- Letters and documents sent by fraudsters are usually badly written. Look out for spelling mistakes and poor grammar.
- End contact with anyone you suspect to be a fraudster and do not send them any money.
- If you have given the fraudsters your bank account details, contact your bank immediately. If you have not already done so, do not give the fraudsters your account details.
- If the fraudsters threaten you once you stop co-operating with them, tell the police immediately.

6. Matrix/multi-level marketing and pyramid schemes

"MAKE MONEY NOW!" scream their websites! And do it in your spare time! Earn big money for almost no work! These schemes are promoted through websites offering expensive electronic gadgets as free gifts in return for spending £15-25 on an inexpensive product, such as a mobile phone signal booster.

Consumers who buy the product then join a waiting list to receive their free gift. The person at the top of the list receives his/her gift only after a prescribed number of new members join up. Most on the list will never receive the item.

The voice of banking & financial services

Pyramid schemes offer a return on a financial investment based on the number of new recruits to the scheme. Investors are misled about the likely returns. There are simply not enough people to support the scheme indefinitely.

7. Property investment schemes

Investors attend a free presentation, which aims to persuade them to hand over big sums of money to enrol on a course promising to make them a successful property dealer, usually involving "no money down".

Schemes can involve the offer of buying yet-to-be-built properties at a discount. Other variations include a buy-to-lease scheme where companies offer to source, renovate and manage properties, claiming good returns from rental income. The properties are generally near-derelict and the tenants non-existent.

8. Impersonation/identity fraud

Impersonation fraud occurs when someone assumes your identity to perform a criminal act. Criminals get the information they need to assume your identity from various sources, such as the theft of your wallet, your rubbish or from credit or bank information. They may approach you in person, by phone or on the Internet and ask you for the information.

Tips to avoid impersonation/identity fraud

- Never throw away ATM receipts, credit cards, or bank statements in a usable form.
- Never give your credit card number over the telephone unless you make the call.
- Reconcile your bank account monthly and tell your bank of discrepancies immediately.
- Keep a list of phone numbers to report the loss or theft of your wallet, credit cards, etc.
- Report unauthorised financial transactions to your bank, credit card company and Police as soon as you detect them.
- Review a copy of your credit report at least once a year. Notify the credit bureau of any questionable entries and follow through until they are explained or removed.
- If your identity has been assumed, ask the credit bureau to print a statement to that effect in your credit report.

For further information see BBA leaflet “Protecting Yourself from Identity Fraud”, available at www.bba.org.uk

The voice of banking & financial services

9. Investment-related scams

“Ponzi" schemes

A Ponzi scheme is an investment fraud in which the operator promises high financial returns or dividends that are not available through traditional investments. Instead of investing victims' funds, the operator pays "dividends" to initial investors using the principle amounts "invested" by subsequent investors. The scheme generally falls apart when the operator flees with the proceeds, or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends".

This type of scheme is named after Charles Ponzi, who operated a scheme in which he guaranteed investors a 50 per cent return on their investment in postal coupons. He was able to pay initial investors but the scheme dissolved when he was unable to pay those who entered later. A recent case of a Ponzi scheme was that run by Bernard Madoff.

Tips to avoid Ponzi schemes

- Exercise due diligence in selecting investments and the people with whom you invest.
- Make sure you fully understand the investment before you invest your money.

Pyramid schemes

Pyramid schemes, also referred to as franchise fraud or chain referral schemes, are frauds in which an individual is offered a distributorship or franchise to market a product. The real profit is earned by the sale of new distributorships, not by the sale of the product. Emphasis on selling franchises rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses.

Tips to avoid pyramid schemes

- Be wary of schemes that require you to bring in subsequent investors to increase your profit or recoup your initial investment.
- Independently verify the legitimacy of any franchise or investment before investing.

10. Letter of credit fraud

Legitimate letters of credit are issued by banks to ensure payment for goods shipped in connection with international trade. These are never sold or offered as investments.

The voice of banking & financial services

Payment on a letter of credit generally requires that the paying bank receive documents certifying that the goods have been shipped and are en route to their intended destination.

Letter of credit frauds are often attempted against banks by providing false documentation to show that goods were shipped when, in fact, no goods or inferior goods were shipped. Other letter of credit frauds occur when con artists offer a "letter of credit" or "bank guarantee" as an investment wherein the investor is promised huge interest rates. Such investment "opportunities" do not exist. (See Prime Bank Notes for additional information.)

Tips to avoid letter of credit fraud

- If an "opportunity" appears too good to be true, it probably is.
- Do not invest in anything unless you understand the deal. Con artists rely on complex transactions and faulty logic to "explain" fraudulent investment schemes.
- Do not invest or try to "purchase" a "letter of credit". Such investments do not exist.
- Be wary of any investment that offers the promise of extremely high yields.
- Independently verify any investment, including the parties involved.

11. Prime bank note fraud

This is a scheme that offers extremely high yields in a relatively short time. Fraudsters purport to have access to "bank guarantees" which they can buy at a discount and sell at a premium. By reselling them several times, they claim to be able to produce exceptional returns. Con artists often say the "guarantees" have been issued by the world's "prime banks" and use terms such as "prime bank notes" and "prime bank debentures". Victims are often required to enter into nondisclosure and noncircumvention agreements. Schemes will often offer returns on investment in "a year and a day", and claim to use forms required by the International Chamber of Commerce (ICC). In fact, the ICC has warned that no such investments exist. While banks use instruments called "bank guarantees" to insure payment for goods in international trade, such bank guarantees are never traded or sold on any kind of market.

Tips to avoid prime bank note related fraud

- Be wary of any scheme that offers unusually high yields by buying and selling anything issued by "prime banks".
- Perform due diligence. Verify the identity of the people, the veracity of the deal, and the existence of the security.
- Be wary of deals that require nondisclosure or noncircumvention agreements that are designed to prevent you from independently verifying details about the investment.