THE POLICE CRIME PREVENTION INITIATIVES

FRAUD GUIDE
Advanced Fee Fraud

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

POLICE CPI
Police Crime Prevention Initiatives

Introduction

This guide is one of a series of guides produced by Police Crime Prevention Initiatives (Police CPI) on behalf of the Mayor's Office for Policing and Crime (MOPAC). These guides form an important element of a larger project which seeks to increase understanding about the various types of fraud and in doing so improving awareness and making people less vulnerable to falling victim to these scams.

Unusually, this project brings together skills and experience of a retired Detective Chief Superintendent from the Metropolitan Police, working with a reformed fraudster, thus providing a unique insight into the tradecraft and methodology of fraudsters.

Contents

Fraud, so what's the problem?

Fraud is the most common form of crime in England and Wales, accounting for 40%+ of recorded offences.

The Crime Survey for England and Wales (CSEW) for the year ending March 2023 estimated that there were 3.5 million fraud offences[1] committed in the previous 12 months, with the UK Finance Annual Fraud Report recording that over £1.2 billion was stolen through fraud in 2022, with much fraud initiated from criminal activity taking place through online platforms and telecommunications[2]. There was a 549% increase in advance fee fraud, from 60,000 to 391,000 offences accordong to the CSEW[3].

1. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023#fraud
2. https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023
3. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023

So, what is Advanced Fee Fraud?

In a nutshell, this type of fraud involves the fraudster using their powers of persuasion to convince the victim to pay in advance for something that doesn't actually exist. This can be anything from a cute puppy, an expensive piece of jewellery, or even something as mundane as a food mixer. At particular times of year, such as in the run-up to Christmas, this type of fraud is rife.

Social media platforms and auction sites are popular hunting grounds, as the fraudster knows that people who shop here have an eye for a bargain and often want to pay as little as possible for gifts they wish to buy for friends and family.

The fraud operates by encouraging victims to make decisions with their hearts rather than their heads.

How does this type of fraud actually work?

Typically, the fraudster advertises something that is in great demand. This could be a children's toy that is in short supply or a fashion item that always attracts a premium price.

In this case let's imagine it's a white gold bracelet from an internationally known fashion house, that normally retails at around £7,500. The fraudster copies a number of photographs from the official website and adds some particularly persuasive wording, ***'I bought this for my ex-girlfriend. I've never even taken it out of the box. We have since split up and I need to move on. Selling this will help me. I have all the papers and the original packaging. Grab a bargain because I just want rid of it as soon as possible. Quick sale £5,000'***

This wording suggests that the seller is offering it at a bargain price if the buyer moves fast. The buyer sees this as a genuine opportunity to either buy it for themselves, or a loved one – or even sell it on and make a profit. In reality, the fraudster is cleverly manipulating the buyer into thinking that they have stumbled across an offer that they cannot afford to pass up.

The fraudster sits back and waits for the messages to start flooding in. Sure enough, within minutes, he starts receiving enquiries. The fraudster doesn't respond straight away, as that might appear a little too eager. Instead, he waits until the evening and copies something akin to the following to all the responses he has received ***'I've been overwhelmed by not only the number of responses to my advert, but also the empathy shown to me regarding my break-up. Thank you for your interest but I've agreed to sell the bracelet to the person who responded first'.***

Those receiving this message are very disappointed but often send a nice reply, hoping that they will be his chosen standby buyer should the original sale fall through. What the fraudster is actually doing, is making the elusive bracelet even more attractive, by dangling the opportunity to buy it, then snatching it away, and emphasising the need to respond quickly.

Next morning, all the prospective buyers receive the same message from the fraudster.

'It turns out that my buyer was a scammer, so I have refused to sell the bracelet to them. It's yours but only if you can pay today'. This puts pressure on the buyer(s). The fraudster has demonstrated that he won't be messed about, he expects a prompt decision and that he won't be scammed again. In doing so, he is also suggesting that he must be a genuine seller.

This is a numbers game. There could be 50 people after this bracelet and they believe that they are the only one to have received this message. The fraudster advises them that he will only take a bank transfer and he will meet them at Liverpool Street Station at 6pm. He provides his account details, his phone number, which is a burner phone – a cheap

phone purchased with prepaid minutes and without a formal contract with a communications provider. This enables fraudsters to use the phone for illicit purposes and reduce the opportunities for it to be traced. He also asks the potential victim to send him a selfie so he can recognise them when they meet, as there are a lot of scammers around! Once again, these conditions are there to reinforce the fact that he is genuine and trustworthy. Of the 50 people who wanted to buy the bracelet, maybe five will transfer the £5,000. This money goes into an account and is moved to another account immediately. The others presumably believed it was too good to be true. How right they were.

At 6pm that night, five people gather at the agreed spot at Liverpool Street Station, all looking for a guy carrying a red leather box containing an expensive bracelet. **Spoiler alert - he's not coming!**

In this case, the fraudster has made £25,000 for a couple of hours work whilst sitting on his sofa with his laptop. His IP address is masked by a Virtual Private Network (VPN) and he throws away the cheap burner phone and SIM card. He has laid out less than £100 and is ready for another day's work tomorrow.

Even if the buyer(s) report this to police and/or Action Fraud, there are few realistic investigative opportunities and many victims don't bother reporting it at all - fewer than a third of victims (32%) report fraud to the authorities, according to research released by National Trading Standards (NTS)[4], with many victims feeling too embarrassed to even tell a relative or friend.

4. https://www.nationaltradingstandards.uk/news/19-million-lose-money-to-scams-but-fewer-than-a-third-report/#:~:text=NTS's%20research%20showed%20that%20when,did%20not%20tell%20their%20bank

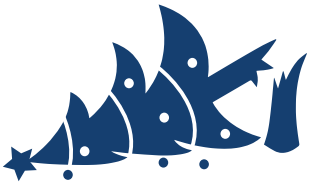
What can you do to protect yourself from becoming a victim to this type of scam?

As mentioned earlier, this fraud operates by encouraging victims to make decisions with their hearts rather than their heads. Looking back at your own experiences can be useful, as often some of our worst decisions were those made when our emotions took over and common sense was forgotten about.

Make your decisions using common sense, not through the desire to grab an unbelievable bargain or through greed

The old adage of 'if it looks too good to be true – it probably is' still rings true

Don't fall for 'sob-stories' it really doesn't matter why they are selling something

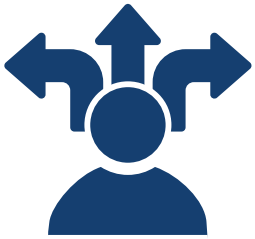


Don't ruin Christmas, birthdays or other celebrations by becoming the victim of scams such as these

Sellers who will only deal with you if you pay in advance are suspicious

Never pay money in advance. Pay cash on collection or use an escrow service such as PayPal or even pay via your credit card which may give you some protection

Trust your own gut instinct. If you have an inner voice advising you to walk away, do so!



Use your head to make decisions, NOT your heart!

What you should do if you if you believe you have been scammed

If the scam is still in progress, or the suspect is known or can be easily identified, or the crime involves a vulnerable victim – call 999 and report it to police immediately.

Otherwise report the scam to Action Fraud (www.actionfraud.police.uk or telephone 0300 123 2040) and contact your own bank immediately if money was transferred to pay for the goods or services.

Whilst investigative opportunities may not be obvious, its vital that the scale and tactics used by fraudsters are understood to assist in identifying patterns and trends. Secure and save any emails and/or texts between yourself and the fraudster. These could provide valuable evidence for investigators.

Tell your friends and family what has happened. Whilst you might feel a little embarrassed, it is incredibly valuable information that can help to stop them becoming a victim of this type of fraud too.

Other Useful Contacts

CIFAS is the UK fraud prevention service, provides protective registration for people who have been victims of fraud or who are considered to be at risk of identity theft.

Citizens Advice Bureau (CAB) provides free, independent and confidential advice in relation to a range of issues www.citizensadvice.org.uk or 0344 111444

Companies House provides free details regarding company ownership www.gov.uk/government/organisations/companies-house

Crimestoppers an independent charity to which you can provide information (anonymously if you wish) regarding crime www.crimestoppers-uk.org

Cyber Aware provides cyber security advice for both individuals and small businesses www.ncsc.gov.uk/cybersaware

Don't be Fooled a partnership between UK Finance and CIFAS to inform students and young people about the danger of becoming Money Mules by sharing their bank details to allow criminals to use their accounts to move and launder money www.moneymules.co.uk

Friends Against Scams a National Trading Standards Scams Team initiative to prevent and protect people from becoming victims of scams www.friendsagainstscams.org.uk

Get Safe Online working with the Metropolitan Police and others, it provides online safety advice for individuals and small businesses www.getsafeonline.org

Hourglass provides a confidential freephone helpline for those who are concerned about, or might have witnessed abuse, neglect or financial exploitation www.hourglass.org or 080 8808 8141

Mail Preference Service is a free service enabling UK consumers to stop receiving unsolicited mail by having their home address removed from mailing lists wwwmpsonline.org.uk or 0207 291 3310

Metropolitan Police Cyber Protect is the Met's Cyber Protect Team provides free products and services to help protect businesses, organisations and individuals from fraud and cybercrime www.met.police/cyberprotect

Metropolitan Police Fraud the fraud pages of the Metropolitan Police website www.met.police.uk/fraud

Metropolitan Police Little Media Series a central store of all the booklets, leaflets and videos created by the Metropolitan Police to assist in raising awareness of fraud and cybercrime www.met.police.uk/littlemedia

Royal Mail Scam Mail if you think you are a family member are receiving scam mail you can report it to Royal Mail at Royal Mail at Freepost Scam Mail, or 0800 011 3466 or via email

Safer Jobs a Metropolitan Police initiative to protect job seekers and agency workers www.safer-jobs.com

Stay Safe Online is Powered by the National Cyber Security Alliance building strong public/private partnerships to create and implement broad-reaching education and awareness.

Take Five to Stop Fraud is a national campaign offering straightforward and impartial advice to help everyone protect themselves from fraud www.takefive-stopfraud.org.uk

Telephone Preference Service (TPS) a central opt-out register allowing individuals to register their wish not to receive unsolicited sales and marketing calls.

The Silver Line operates the only free confidential helpline for older people in the UK. It is available 24 hours a day, 7 days a week www.thesilverline.org.uk or 0800 470 8090

Think Jessica is a charity set up to protect elderly and vulnerable people from scams which come through the postal system and/or criminals who contact them by telephone www.thinkjessica.com

National Trading Standards is responsible for gathering important intelligence from around the country to target rogue traders, mass-marketing and internet scams that go beyond local authority boundaries www.nationaltradingstandards.uk or 0808 223 1133

Age UK is the country's largest charity dedicated to helping everyone make the most of later life www.ageuk.org.uk or 0800 169 8787

Police Crime Prevention Initiatives (Police CPI)

Police CPI works to deliver a wide range of innovative and ground-breaking crime prevention and demand reduction initiatives to support the wider UK Police Service, central and local government and the general public.

Part of the National Police Chiefs' Council Prevention Coordination Committee, Police CPI works closely with government, manufacturers and companies involved in security products (within the UK and those in countries that supply the UK), standards authorities and key stakeholders such as Planners, Architects, Developers, Local Authorities, Housing Associations, academia and the public.

Police CPI is a not-for-profit police owned organisation, self-funded through its prevention activities. Senior police officers from England, Scotland, Wales and Northern Ireland control and direct the work Police CPI carries out on behalf of the Police Service.

Mayor's Office for Policing and Crime (MOPAC)

The Police Reform and Social Responsibility Act 2011 established a Police and Crime Commissioner (PCC) for each police force area across England and Wales. In London, the elected Mayor is the occupant of the Mayor's Office for Policing and Crime (MOPAC).

MOPAC has a dedicated team including specialists in commissioning, finance, oversight, policy, professional standards, research and analysis, community engagement and auditing. Together, they work to deliver the Mayor's Police and Crime Plan and make London a safe city for all.

Police Crime Prevention Initiatives

2nd Floor, 50 Broadway, St James's Park
Westminster, London, SW1H 0BL

Tel: 0203 8623 999

Email: enquiries@police-cpi.co.uk

Web: www.policecpi.com

MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

POLICE CPI
Police Crime Prevention Initiatives