Hillingdon Cyber Crime Summary
May 2022

Executive Summary

Number of offences	154
Total loss	£395,214.19
Average per victim	£2,566.33

Top 5

The top 5 by **volume** (number of reports) type of fraud is as follows:

Fraud Type	Amount of Offences	Amount Lost
NFIB3A - Online Shopping and Auctions	31	£14,111.53
NFIB1H - Other Advance Fee Frauds	20	£13,796.58
NFIB3D - Other Consumer Non Investment Fraud	12	£23,012.32
Push Payment	11	£58,394.31
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	9	£40,845.24

The top 5 by **amount** reported lost:

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£153,882.70	8
Push Payment	£58,394.31	11
NFIB1D - Dating Scam	£42,455.00	6
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£40,845.24	9
NFIB3D - Other Consumer Non Investment Fraud	£23,012.32	12

Fraud Advice

Investment Fraud

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Fraudsters will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Common products that will be offered include binary options, virtual currency, carbon credits, wine, rare metals, gemstones, land and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised and they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.
Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's status. However, fraudsters are also aware of this and exploit it. The fraudster may put pressure on you by offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit.

In addition - be wary of companies that offer to 'recover' any funds you have lost to any sort of investment scam. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'Recovery Fraud'.

How to protect yourself

- There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
- Before investing, check the Financial Conduct Authority register to see if the firm or individual you are dealing with is authorised (https://register.fca.org.uk/)
- Check the FCA Warning List of firms to avoid.

REMEMBER - Don't be pressured into making a quick decision.

CAUTION - Seek independent financial advice before committing to any investment.

THINK - Why would a legitimate investment company call me out of the blue?

Romance and Dating Fraud

Dating online is now one of the most popular ways for new couples to meet, with millions of people finding new relationships, romance and love this way. Unfortunately, amongst the genuine profiles are fake profiles set up by fraudsters. They are after your money, not your love. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.

Criminals will build a relationship with online members, quickly asking to move communication off the dating website. This is so they can continue their contact with you, even if their profile is later identified by the site as fraudulent and subsequently deleted.

Fraudsters are often very flattering, appearing really interested in you within a short space of time. However, they will use a range of excuses as to why they can't meet in person, such as they are stuck overseas, have a family emergency or have an issue with their business. They then start asking for money to help with their problems, assuring you they will pay it back as soon as they can. The fraudster may claim to be desperate to meet you as soon as this obstacle is overcome. This is all a scam and their true intention is to take as much money from you as they can.

How to Protect Yourself

- Stay on site.
- Keep all communication on the dating website you are using. Don't be convinced by profile pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like https://www.tineye.com or https://reverse.photos

- Do your own research on the person – are they members of any other social networking sites? Can you confirm what they are telling you about themselves, such as where they work or where they live?
- Never send money to someone you have not met in person and be extremely wary of giving money to someone you have recently started a relationship with.
- Be wary of anyone asking you to receive money on their behalf and transfer it on. They may be using you to launder money.
- Talk to family and friends for advice, even if the other party is asking you to keep the relationship secret.
- Watch our video on Romance Fraud at www.met.police.uk/littlemedia

REMEMBER - Stay on site! Never send money to someone you have not met in person, or receive/ transfer money on their behalf.

CAUTION - Be wary of continuing the relationship away from the dating website you initially made contact on.

THINK - Why are they so quick to declare their love for me? How do I know they are telling me the truth?

Advance Fee Fraud

Advance Fee Fraud is an umbrella term to describe a particular fraud type where the criminal convinces a victim to make upfront payments for goods, services and/or financial gains. But the goods/services don't exist.

Many different types of Advance Fee Fraud using various techniques and scams are used by criminals. Some of these (including Romance Fraud and Recruitment Fraud) are covered more in-depth later in this book. However, the numerous different tactics used by criminals means it's worth describing the basic technique behind the fraud; the criminal will offer something to you, but in order to progress, you'll need to pay something up front. Below is a list of types of Advance Fee Fraud. This list is by no means exhaustive!

Clairvoyant or Psychic Fraud– The criminal predicts something significant in your future, but they need money to provide a full report.

Cheque Overpayment Fraud – The criminal overpays for something with an invalid cheque, and asks for change.

Fraud Recovery Fraud – Once you've been a victim of fraud, the criminal contacts you, claiming that they can recover your losses, for a fee.

Inheritance Fraud – The criminal tells you that you're in line to receive a huge inheritance, but you'll need to pay a fee to release the funds.

Loan Fraud– The criminal asks you to pay an upfront fee for a loan.

Lottery Fraud – You're told you've won a prize in a lottery, but you'll need to pay the criminal an admin fee.

Racing Tip Fraud – The criminal offers racing tips that are "guaranteed" to pay off, for a small fee.

Rental Fraud – The criminal asks for an upfront fee to rent a property, which may not be theirs, or even may not exist.

Hillingdon Cyber Crime Summary
May 2022

West African Letter Fraud (aka 419 Fraud) – The criminal asks for help moving a large sum of money from one country to another, promising to cut you in, but asks for a payment upfront first.

Work from home Fraud – The criminal offers you to make easy money working from home, but you need to pay a fee in advance, for business leads, or a website.

Vehicle Matching Fraud – The criminal contacts you just after you've placed an advert trying to sell something (usually a car). They ask for a "refundable" fee to put you in touch with a non-existent immediate buyer.

How to protect yourself

- Be extremely wary about giving money to anyone upfront, especially a stranger, for any reason.
- If they claim to be an official, double check their identity, but don't do so using any contact details they give you.
- Don't be pressurised into making a decision in that moment. Always take time to think, don't forget to Take 5.

REMEMBER – Criminals will try any lie to get your money

CAUTION – Don't give money upfront if you have even the slightest suspicion

THINK – Why should I give this person money? Why have they targeted me?

Remember:

Your bank, the police, or tax office will **never** ask you to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers.

This is a scam.

1. **Hang up** (Never give details or money following a cold call)
2. **Take 5** (Seek a second opinion, tell someone what has happened)
3. **Verify** (if concerned, contact the company via a pre-confirmed method)

All of our videos and electronic leaflets can be found on the following link;
www.met.police.uk/littlemedia

Free cyber advice can be found https://www.ncsc.gov.uk/cyberaware/home

Always report, Scams fraud and cyber crime to Action Fraud, either online at **www.actionfraud.police.uk** **or by telephone on 0300 123 2040.**

STOP
Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE
Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT
Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.