Croydon Cyber Crime Summary
May 2023

Executive Summary

Number of offences	236
Total loss	£721,032.20
Average per victim	£3,055.22

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	43	£24,368.33
NFIB1H - Other Advance Fee Frauds	24	£47,370.00
NFIB3D - Other Consumer Non Investment Fraud	23	£150,190.45
NFIB52C - Hacking - Social Media and Email	16	£0.00
NFIB2E - Other Financial Investment	13	£159,201.84

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£159,201.84	13
NFIB3D - Other Consumer Non Investment Fraud	£150,190.45	23
NFIB19 - Fraud by Abuse of Position of Trust	£110,787.90	2
NFIB3E - Computer Software Service Fraud	£109,159.00	6
NFIB1H - Other Advance Fee Frauds	£47,370.00	24

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?

Fraud by Abuse of Position of Trust

When someone abuses their position of authority or trust for personal or financial gain, or so that someone else loses money or status.

Friends, family members, carers or company employees may be asked to look after your personal or business finances. They may instead take advantage of their access to bank accounts or information for their own benefit, or misuse the assets of a business to embezzle funds for themselves.

How to Protect Yourself

- Make sure you have complete confidence in anyone you entrust with your finances to make decisions on your behalf. Don't be afraid to change your mind in future.
- Grant the trust to more than one person to make joint decisions (so everyone in the position of trust has to agree on decisions together).
- You'll need to be prepared to challenge suspicious behaviour if you've been given a position of trust alongside someone else.
- If you're being pressured into making a decision by someone you've given a position of trust to or being intimidated or told to keep certain dealings secret from other trustees, then make sure you speak to someone else you trust.

Computer Software Service Fraud

Criminals may cold call you claiming there are problems with your computer and they can help you to solve them. They often use the names of well-known companies such as Microsoft, Apple or Amazon. They may even use the name of your broadband provider to sound more legitimate.

The criminals may ask you to complete a number of actions on your computer, and they may even be able to demonstrate an 'error'. They'll then usually instruct you to download what is known as a 'Remote Access Tool'. This gives the criminal access to everything on your computer. They can access and copy your data, or download malware onto your computer to monitor what you do in the future.

Fraudsters can even access your online banking, and transfer money between your accounts.
You may also be asked to pay for the 'assistance' you have been given. This could be a one-off payment or an ongoing direct debit over many months/years. If you do provide payment details, these may be used to commit further fraud against you.

How to protect yourself

- A genuine computer service company will never call you out of the blue regarding issues with your computer. If you receive a call like this hang up straight away.
- Never allow anyone to remotely access your computer.
- If you are having issues with your computer, contact the retailer you purchased it from regarding service and repair. If you are having issues with your internet speed or service, contact your service provider for advice or support.
- Most broadband providers offer a free and easy test to measure the speed of your broadband service.
- Watch our video on Computer Software Service Fraud at **www.met.police.uk/littlemedia**

REMEMBER - Genuine computer service companies don't make these calls.
CAUTION - Don't let anyone remotely access your computer.
THINK - Why are they calling me, there didn't seem to be a problem? How do I know they are genuine?

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.