

Hillingdon Cyber Crime Summary

January 2025

Executive Summary

Number of offences	147
Total loss	£760,369.76
Average per victim	£5,172.58

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB1H - Other Advance Fee Frauds	19	£27,356.76
NFIB3A - Online Shopping and Auctions	19	£33,207.65
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	13	£21,180.41
NFIB52C - Hacking - Social Media and Email	9	£0.00
NFIB2E - Other Financial Investment	8	£274,629.00

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£274,629.00	8
NFIB2B - Pyramid or Ponzi Schemes	£266,221.90	6
NFIB3D - Other Consumer Non Investment Fraud	£39,180.00	7
NFIB3A - Online Shopping and Auctions	£33,207.65	19
NFIB1E - Fraud Recovery	£32,028.06	3

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.

Hillingdon Cyber Crime Summary

January 2025

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?

Pyramid or Ponzi Schemes

Pyramid scheme fraud involves an unsustainable business which rewards people for enrolling others into a business that offers a non-existent or worthless product.

A fraudster advertises a multi-level investment scheme that offers extraordinary profits for little or no risk. You're required to pay a fee to enter the investment scheme.

You're then required to recruit friends or family members to enter the scheme. If you do this successfully, you're paid out of their receipts. They are then told to recruit others to keep the chain going.

Your money is not actually invested in any product. Instead, it's simply passed up the chain of investors. Because pyramid schemes are unauthorised and make no profits, you're very unlikely to recover any lost investment. While the fraudster at the top will collect most of the profits, those who entered the scheme later end up losing out. Legitimate trading schemes rely on valuable goods and services, while illegal pyramid schemes focus simply on recruiting more and more investors.

Using hard-sell techniques, fraudsters try to pressure you into making rushed decisions, giving you no time to consider the nature of the investment.

Fraudsters aim to make their business seem legitimate. This means they will often use technical jargon, impressive job titles and mock websites to look credible. If you have any suspicions about a scheme's authenticity, you should investigate the company's status and contact details.

How to Protect Yourself

- If you're considering any type of investment, always remember: if it seems too good to be true, it probably is. High returns can only be achieved with high risk.
- Pyramid schemes often involve products that are overpriced and have no real resale value. You should think about the true

Hillingdon Cyber Crime Summary

January 2025

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.
- **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.

Hillingdon Cyber Crime Summary

January 2025

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>

- **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.

Where to Report a Scam:

If you think you have been scammed, contact your bank first by calling 159

How it Works; 159 works in the same way as 101 for the police or 111 for the NHS. It's the number you can trust to get you through to your bank safely and securely every time. So if you think someone is trying to scam you into handing over money or personal details – stop, hang up and call 159 to speak directly to your bank.

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

Subscribe to the “**Which**” Scam Alert Service where you can receive free updates on current scams being used. Copy this link into your search engine <https://act.which.co.uk/> and locate “Scam Alerts newsletter” to register your details. **Which** will then provide practical advice to keep you one step ahead of fraudsters.

Get advice and report it to Trading Standards through the Citizens Advice consumer service on 0808 223 1133 or online advice at www.adviceguide.org.uk

The Citizens Advice consumer service provides free, confidential and impartial advice on consumer issues. It is important that all complaints are referred to the Citizens Advice consumer service as they maintain a national database of complaints that provides an invaluable source of information and intelligence to the trading standards community

Details of all consumer enquiries, dealt with by the Citizens Advice consumer helpline, are made available to Trading Standards

Report a text message you think is a scam - most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.

Report an email you think is a scam - If you have received an email which you're not quite sure about, forward it to report@phishing.gov.uk

Hillingdon Cyber Crime Summary

January 2025

If you've been scammed through the post - Royal Mail investigates postal scams. If you've received something in the post you think is a scam, send it to '**Freepost Scam Mail**'. Include the envelope it came in and a completed scam mail report. You can download a scam mail report from Royal Mail or call them and ask for a form and pre-paid envelope

If the scam involves financial services - If the scam involves cryptocurrency, investments, insurance or pensions, report it to the **Financial Conduct Authority - 0800 111 6768**

Friends Against Scams is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.

Online learning available

<https://www.friendsagainstscams.org.uk/training/friends-elearning>



**METROPOLITAN
POLICE**

