

Hillingdon Cyber Crime Summary

February 2025

Executive Summary

Number of offences	140
Total loss	£687,576.29
Average per victim	£4,911.26

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB52C - Hacking - Social Media and Email	20	£0.00
NFIB1H - Other Advance Fee Frauds	16	£21,426.44
NFIB3A - Online Shopping and Auctions	13	£14,009.65
NFIB3D - Other Consumer Non Investment Fraud	13	£7,674.19
NFIB52B - Hacking - Personal	12	£0.00

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2A - Share sales or Boiler Room Fraud	£403,543.77	2
NFIB2E - Other Financial Investment	£119,950.00	5
Push Payment	£36,558.18	6
NFIB3E - Computer Software Service Fraud	£35,270.28	3
Courier Fraud	£22,052.68	2

Fraud Advice

Share Sales or Boiler Room Fraud

Fraud by false representation – The fraudster dishonestly makes a false representation and intends to make a gain for himself (or another), cause loss to another or expose another to risk of loss.

Share/bond Sales or Boiler Room Fraud “Boiler room fraud is a fraud where victims are cold-called by fake stockbrokers and encouraged or persuaded to buy shares or bonds in worthless, non-existent or near bankrupt companies.” Boiler room is the term used for the illegal offshore dealing rooms that are often located abroad in Spain, Switzerland or the USA. The sales person cold calls potential victims and oppressively sells shares or bonds that are non-existent or worthless enticing victims with the promise of quick, high returns on the investment. In a bid to appear legitimate, a Boiler room may have a web-site and produce glossy literature and use a telephone number with a London prefix that diverts overseas.

How to Protect Yourself

- Look into the company offering the investment scheme thoroughly. Find as much independent information as you can by using the websites of regulators, such as the FCA. Don't trust anything you see on any website or social media to which the company directs you.
- Always double check.
- Choose regulated firms who have the right licences such as the Markets in Financial Instruments Directive (MiFID) and the Insurance Distribution Directive (IDD).
- Be wary of promotional material that promises great returns without much detail.
- Lots of existing investors or friends and family investing does not mean it's not a scam. It just means there are lots of victims, some of whom you know.

Hillingdon Cyber Crime Summary

February 2025

- Criminals will encourage you to make hurried decisions and may use technical jargon designed to baffle and confuse. They may also tell you there is a deadline in order to invest or be included due to high demand.

Ask simple questions about the company and scheme and be very wary if they dodge the questions or are unable to provide clear answers with supporting documentation.

Push Payment Fraud

Online banking makes managing money easier for the general public, however criminals are taking advantage of this ease of banking and using it to defraud the public.

Criminals can pretend to be from somewhere official, for example, your bank, or the tax office. They contact you via email, phone or social media, and then warn you of fake suspicious or criminal activity on your bank account. They state that they've set up a safe account for you to transfer your funds into. However, this is actually their account.

How to protect yourself

- Be suspicious of a call out of the blue from someone claiming to be from a position of authority.
- Take down the person's details (name, authority, department, branch etc.) and verify using independent source contact details.
- A genuine official from the Police, your bank, HMRC or any other trusted authority will NEVER call you to ask you to verify your personal banking details, PIN or password, or threaten you with arrest.
- Never transfer money into another account unless you are 100% certain of the owner of the account.
- Your bank will never set up a "safe" account for you.
- If you are a victim, contact your bank as soon as possible, as they may be able to help stop the transfer.
- Watch our video on Impersonation Fraud at www.met.police.uk/littlemedia.

REMEMBER – Your bank will never set up a "safe account".

CAUTION – Unless you definitely know who the account belongs to, it might not be safe.

THINK – Who told me this account was safe? Have I checked their identity?

Social Media & Email Hacking

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

You can improve your cyber security by taking six actions:

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

Hillingdon Cyber Crime Summary

February 2025

More information and cyber advice can be found here;

<https://www.ncsc.gov.uk/cyberaware/home>

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>

- **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

Hillingdon Cyber Crime Summary

February 2025

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**

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**

