Havering Cyber Crime Summary
December 2023

Executive Summary

Number of offences	137
Total loss	£455,397.42
Average per victim	£3,324.07

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	27	£18,584.09
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	14	£136,783.52
NFIB52C - Hacking - Social Media and Email	14	£0.00
NFIB1H - Other Advance Fee Frauds	12	£15,726.00
NFIB3D - Other Consumer Non Investment Fraud	9	£8,052.20

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

Fraud Type	Amount Lost	Amount of Offences
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£136,783.52	14
NFIB2E - Other Financial Investment	£131,200.00	2
NFIB2B - Pyramid or Ponzi Schemes	£52,837.00	8
Push Payment	£40,321.42	7
NFIB52E - Hacking Extortion	£20,000.00	2

Fraud Advice

Banking and Card Fraud - Online Banking

The use of online banking or people using banking apps on smartphones and tablets has grown. People use them at home or when they are out and about.

To stay safe while banking online you must protect your password and personal details to stop criminals from accessing your accounts. Many banks provide one-time passcodes sent to your device when setting up new payments. These should never be shared with anyone, even from the bank. If you're speaking to your bank on the phone, and they ask you for it, you are certainly speaking to a criminal, not your bank.

How to protect yourself

- Choose, use and protect passwords and memorable words with great care. Watch our video on passwords at www.met.police.uk/littlemedia for further advice.
- Keep online banking software and banking apps up to date. Always download updates when prompted.
- When logging in whilst in public, take extra care to shield any PIN codes or passwords.
- Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- Do not use publicly available Wi-Fi networks for banking. It is very difficult to tell if a hotspot is secure.
- Don't share any security codes with anyone.

If your bank has called you. Take a reference number, and then hang up before recalling on a number you know to be safe after a few minutes to clear the line.

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

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?

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.