Havering Cyber Crime Summary
October 2022

Executive Summary

Number of offences	97
Total loss	£276,709.14
Average per victim	£2,852.67

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	23	£4,892.64
NFIB1H - Other Advance Fee Frauds	11	£4,871.25
NFIB3D - Other Consumer Non Investment Fraud	8	£25,223.99
Push Payment	7	£20,566.00
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	6	£22,359.95

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

Fraud Type	Amount Lost	Amount of Offences
NFIB19 - Fraud by Abuse of Position of Trust	£150,000.00	1
NFIB3D - Other Consumer Non Investment Fraud	£25,223.99	8
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£22,359.95	6
NFIB3C - Door to Door Sales and Bogus Tradesmen	£20,704.00	3
Push Payment	£20,566.00	7

Fraud Advice

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.

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.

Door-to-Door Fraud

Door-to-door scams involve criminals knocking on your door and unexpectedly offering products or services. Fraudsters convince you to pay for goods or work which is often overpriced, of poor quality or is not even carried out. In many cases, this work is not necessary. They may use intimidation and pressure you to make quick decisions so that you agree to their demands.

Criminals may try to convince you that work is urgently required and the price they are charging is fair. They will put pressure on you to have the work done immediately and may ask for payment upfront. Often the work is not completed, or if it is, the work is to a poor standard. You may also be overcharged for any work done.

They can use deception to convince you:

- Claiming they were working on a neighbours' address and noticed you need work completed and they have left over materials.
- They may inspect areas you can't access, for example the loft or roof and show you photos or videos claiming they are evidence that you need the urgent repairs. Beware of these tactics as these images may not even be your property.

- They may throw water down when you are not looking to indicate you have 'damp'.

- They may be insistent you pay in cash immediately or put down a deposit, even offering to take you to the bank to get the money. If you do this, they may continue to find reasons for you to pay more money.

- Some callers will be legitimate. Gas, electricity and water companies may visit to read your meters. Charities may visit to ask for donations and council officials may contact you regarding local issues. Always ask for identification and tell them to wait outside whilst you check this by calling the company or speaking to a relative or friend. If you are calling the company, don't use the phone number on the person's ID card).

How to protect yourself

- Always check their identity. If you are not happy about a person's identity, do not let them into your house under any circumstances.

- Never leave your front door open/unlocked and unattended, so a second individual can't enter without your knowledge.

- Take time to consider your options and research costs from other providers. If in doubt contact your local Trading Standards.

- If you feel pressured by any cold caller, have the confidence to be firm and say no.

- Call the citizens advice consumer helpline following a doorstep caller on 03454 04 05 06.

REMEMBER - Take time to consider your options. Don't be pressured into making a quick decision.

CAUTION - Never pay upfront for goods or services you have not received.

THINK - Are they a legitimate company? Why haven't they given you a written quote?

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.**

Havering Cyber Crime Summary
October 2022

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.