Havering Cyber Crime Summary
September 2022

Executive Summary

Number of offences	96
Total loss	£276,663.46
Average per victim	£2,881.91

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	19	£11,484.48
NFIB3D - Other Consumer Non Investment Fraud	13	£35,851.20
NFIB1H - Other Advance Fee Frauds	10	£8,776.11
NFIB3F - Ticket Fraud	5	£8,727.74
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	5	£24,586.78

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£127,896.00	3
NFIB3D - Other Consumer Non Investment Fraud	£35,851.20	13
Push Payment	£30,960.16	5
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£24,586.78	5
NFIB3C - Door to Door Sales and Bogus Tradesmen	£13,041.00	2

Fraud Advice

Other Consumer Non Investment Fraud

Sometimes businesses use deceptive business practices that can cause their victims to suffer financial losses.

The victims believe they are participating in a legal and valid business transaction when they are actually being defrauded. Fraud against consumers is often related to false promises or inaccurate claims made to consumers, as well as practices that directly cheat consumers out of their money.

How to protect yourself

- Research the company before purchasing goods or services.
- Use Companies House to find out how long they have been trading.
- Ensure you use trusted, reviewed companies.
- Avoid using direct bank transfers when purchasing items online, instead use a credit card.

Havering Cyber Crime Summary
September 2022

Ticket Fraud

Getting tickets to see your favourite band, football team or theatre production can be extremely difficult as tickets sell out quickly. Criminals take advantage of this by offering tickets for sale that do not exist or are fake.

Most event tickets are sold via reputable websites operated by promoters, the event venue or other official agents. Many tickets are also offered for sale on secondary resale websites, place adverts on secondary resale sites or use social media to sell tickets they do not have.

Once a payment is made you will either not receive the tickets or the tickets you receive will be fake or non-transferrable. When you arrive at the venue you will not get in. Some tickets are non-transferrable and can only be used by the person who initially purchased them. In many cases unauthorised resale of these tickets is illegal.

How to Protect Yourself

- Buy tickets from the event promoter, venue box office, official agent or a reputable ticket exchange site or app.
- Be suspicious of requests to pay by bank transfer. Where possible use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75.
- Be wary of paying for tickets where you are told someone will meet you at the event with your tickets as they may not arrive.
- If the retailer is a member of the Society of Ticket Agents and Retailers (STAR) you are offered additional protection if something goes wrong. If a website shows their logo you can check they are really a member on www.star.org.uk
- For further information on buying tickets safely visit the STAR website.

REMEMBER – The site you are using could be fake.

CAUTION – Use your credit card to pay this could offer you additional protection.

THINK – How can I check the tickets are real?

Online Shopping and Auction Sites

Online shopping can save you time, effort and money. Millions of people use websites such as eBay and AutoTrader to buy new or second hand goods for competitive prices. These sites give you the opportunity to purchase a huge choice of goods from all over the world. However, among the genuine buyers and sellers on these sites, there are criminals who use the anonymity of the internet to offer goods for sale they do not have, or are fake.

In the majority of transactions, the buyer and seller never meet. Which means when making a purchase or sale on a website, you are reliant on the security measures of the site.
Fraudsters will advertise an item for sale, frequently at a bargain price compared to other listings of a similar type. They may have pictures of the item so it appears to be a genuine sale.

A favoured tactic is to encourage buyers to move away from the website to complete the transaction, and the criminal may offer a further discount if you do so. Many websites offer users the opportunity to pay via a recognised, secure third party payment service, such as PayPal, Android Pay or Apple Pay. Read the website's advice and stick to it. Fraudsters might be insistent you pay via bank transfer instead. By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

Criminals may also email or contact you if you have 'bid' on an item but not been successful in winning the auction. They will claim that the winning bidder pulled out or didn't have the funds and offer you the chance to buy the item. Once you agree, they will either provide bank details or even insist payment is made via a third party payment service for mutual protection. Once you agree, they 'arrange' this. You then receive a very legitimate looking email which appears to be from the website or a third party payment service directing you how to make the payment. Some are very sophisticated, even having 'Live Chat' functions that you can use to speak to a sales advisor! Unfortunately, you will again be communicating to the fraudster, so beware!

In both these scenarios, once the payment is made, the 'seller' won't send the item. They'll either not reply to you or make excuses as to why they haven't sent the goods. If they do send the item, they'll send counterfeit goods instead of the genuine items advertised. Again, you may struggle to receive any compensation or resolution to this problem from the legitimate website, as it could be against their policies.

Fraudsters also use e-commerce websites to pose as 'buyers.' If you have an item for sale, they may contact you and arrange to purchase this. It is common for criminals to fake a confirmation that payment has been made. Before posting any item, log in to your account via your normal method (not a link on the email received) and check that you have received the money.

You must also be careful what address you send items to. Fraudsters may ask you to send items to a different address. They may claim they need it sent to their work address or to a friend or family member. If you send the item to an address other than the one registered on the user account, you may not be provided any protection from the website or payment service.

How to protect yourself

- Stay on site!
- Be wary of offers that look too good to be true.
- Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.
- Research the seller/buyer and any of their bidding history.
- Don't be convinced by pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like **www.tineye.com** or **https://reverse.photos/**
- Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.
- Never buy a vehicle without seeing it in person. Ask to see the relevant documentation for the vehicle to ensure the seller has ownership.
- If you are selling online, be wary of any emails stating funds have been sent. Always log in to your account via your normal route (not via link in email) to check.
- Watch our video on Online Shopping Fraud at **www.met.police.uk/littlemedia**.

REMEMBER - Stay on site.

CAUTION - Be wary of paying by bank transfer or virtual currency.

THINK - Why is this item so cheap? Is it a scam?

Havering Cyber Crime Summary
September 2022

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.