

Croydon Cyber Crime Summary

February 2024

Executive Summary

Number of offences	198
Total loss	£303,682.90
Average per victim	£1,533.75

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB3D - Other Consumer Non Investment Fraud	25	£20,121.51
NFIB3A - Online Shopping and Auctions	24	£24,818.44
NFIB1H - Other Advance Fee Frauds	19	£32,781.56
Push Payment	15	£40,751.53
NFIB52C - Hacking - Social Media and Email	13	£0.00

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

Fraud Type	Amount Lost	Amount of Offences
NFIB2E - Other Financial Investment	£55,886.67	7
NFIB52B - Hacking – Personal	£50,000.00	4
Push Payment	£40,751.53	15
NFIB1H - Other Advance Fee Frauds	£32,781.56	19
NFIB3A - Online Shopping and Auctions	£24,818.44	24

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.

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.

Croydon Cyber Crime Summary

February 2024

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?

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.

Croydon Cyber Crime Summary

February 2024

- **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.

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.