Waltham Forest Cyber Crime Summary September 2025

Executive Summary

Number of offences	166
Total loss	£339,971.02
Average per victim	£2,048.02

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	24	£32,118.96
NFIB1H - Other Advance Fee Frauds	20	£18,971.83
NFIB52C - Hacking - Social Media and Email	17	£0.00
NFIB3D - Other Consumer Non Investment Fraud	11	£10,636.34
NFIB3F - Ticket Fraud	10	£13,793.00

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

Fraud Type	Amount Lost	Amount of Offences
Courier Fraud	£84,057.41	2
NFIB2E - Other Financial Investment	£76,263.09	8
NFIB3A - Online Shopping and Auctions	£32,118.96	24
NFIB3E - Computer Software Service Fraud	£28,086.00	3
NFIB1H - Other Advance Fee Frauds	£18,971.83	20

Fraud Advice

Courier Fraud

Fraudsters cold call you pretending to be from your bank or from the police. They claim there is an issue with your bank account or request your assistance with an ongoing bank or police investigation.

They claim they are conducting an investigation, often saying it involves corrupt bank employees or police and ask for your help or say your account is at risk. The ultimate aim of this call is to trick you into parting with your money either in person, online, via a money service bureau or in a bank. If they manage to convince you, they instruct you to carry out a task which ultimately involves you handing over your money. These include:

- Asking you to attend your bank branch to withdraw a large sum of money which they will then collect from you for evidence. They may claim the money may be counterfeit, or that it is going to be sent off for forensic or fingerprint analysis.
- Asking you to withdraw large amounts of foreign currency, which will similarly be collected by a courier from your home address.
- Asking you to provide details over the phone, including typing in your PIN then handing over your cards to a courier sent to your address (often after you have cut them up as instructed).

- Asking you to purchase high value items, such as expensive watches to 'clear criminal funds' which will again be collected by a courier.

- Asking to purchase other items, like gift cards or vouchers.

In all of these cases they will assure you that you will soon be reimbursed.
Fraudsters want to avoid detection, and may give you instructions to achieve this such as:

- Informing you it is an undercover operation involving bank/police corruption, so you must not tell bank staff or police anything about the phone call. They may even threaten that you could be arrested if you do.

- Give you a cover story to tell bank staff or police, e.g. the money/item is for building works, a holiday or a gift for a relative.

- Criminals have developed their methods further to no longer involve the courier. They may now claim that as a result of the fraud, they are investigating your bank account and therefore ask you to transfer your money into a 'safe account'. They will provide you with the account details and may even say this is set up in your name. This is called *Push Payment Fraud*.

How to protect yourself

- Be extremely wary of unsolicited phone calls from your bank or the police, particularly if they are requesting personal information. End the call, call back on a different phone line or on a mobile. If this is not possible, wait at least one minute before calling back. Use either the telephone number on your bank card, go to the bank's website or for the police dial '101'.
- Speak to friends or family before carrying out any actions. Don't trust claims made by cold callers.
- Never hand over your money, bank cards or make purchases following an unexpected call.
- Never share your PIN with anyone.
- Watch our video on Impersonation Fraud at **www.met.police.uk/littlemedia**

REMEMBER - Your bank or the police will never ask you for your PIN, bank card, or ask you to withdraw money or buy items on their behalf.

CAUTION - If you receive an unexpected call, hang up and use another phone to call back and confirm identity.

THINK - How do I know they are who they say they are?

Investment Fraud

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Fraudsters will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Common products that will be offered include binary options, virtual currency, carbon credits, wine, rare metals, gemstones, land and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised and they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.
Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.

Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's status. However, fraudsters are also aware of this and exploit it. The fraudster may put pressure on you by offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit.

In addition - be wary of companies that offer to 'recover' any funds you have lost to any sort of investment scam. They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'Recovery Fraud'.

How to protect yourself

- There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
- Before investing, check the Financial Conduct Authority register to see if the firm or individual you are dealing with is authorised (**https://register.fca.org.uk/**)
- Check the FCA Warning List of firms to avoid.

REMEMBER - Don't be pressured into making a quick decision.

CAUTION - Seek independent financial advice before committing to any investment.

THINK - Why would a legitimate investment company call me out of the blue?

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.

Waltham Forest Cyber Crime Summary September 2025

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.

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

- **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

Waltham Forest Cyber Crime Summary September 2025

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

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