

# Richmond Cyber Crime Summary

## April 2025

### Executive Summary

Number of offences	99
Total loss	£432,604.24
Average per victim	£4,369.74

### Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB1H - Other Advance Fee Frauds	14	£20,338.81
NFIB52C - Hacking - Social Media and Email	13	£0.00
NFIB3A - Online Shopping and Auctions	11	£11,637.32
NFIB3D - Other Consumer Non Investment Fraud	9	£14,649.06
Push Payment	5	£23,431.67

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

Fraud Type	Amount Lost	Amount of Offences
NFIB5D - Mandate Fraud	£269,000.00	1
NFIB2E - Other Financial Investment	£39,293.67	3
Push Payment	£23,431.67	5
NFIB1H - Other Advance Fee Frauds	£20,338.81	14
NFIB1D - Dating Scam	£19,900.00	3

### Fraud Advice

#### 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.



# Richmond Cyber Crime Summary

## April 2025

- **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.
- **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?

### Social Media & Email Hacking

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

You can improve your cyber security by taking six actions:

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices
6. Back up your data

More information and cyber advice can be found here;  
<https://www.ncsc.gov.uk/cyberaware/home>



**METROPOLITAN  
POLICE**



# Richmond Cyber Crime Summary

## April 2025

### Payment Fraud (aka Mandate Fraud)

**Payment fraud is a specific type of fraud which targets businesses with the intention of getting them to transfer money to a bank account operated by the criminal.**

There are two main types of payment fraud, **CEO fraud** and **Mandate Fraud**. Both are usually targeted at staff within a company's accounts department and use spoofed sender email addresses (sometimes called Business Email Compromise). CEO fraud involves an email that claims to be from a senior member of staff within a company such as a CEO (Chief Executive Officer). The email will ask the receiver to make a payment or transfer funds for an ongoing or new business transaction. Often the payment request is marked as urgent and pressure is applied to the receiver to make the payment as soon as possible.

Mandate fraud involves an email which appears to come from a known supplier. The email will request that future payments for products or services are made to a new bank account and give a reason for the account change. In each instance, the new account will be under the control of the criminal and any funds paid in to it will be lost.

### How to protect yourself

If an email is received requesting a change of bank details on an account or a one off payment, verify this by making direct contact with the organisation or person requesting the change. Ideally, phone them on a number you already have, failing that, double check the email used. Do not use any contact details from the suspicious email. Don't be pressurised by any email, or follow up phone call, as this may be the criminal. Always double check.

However, some criminals are getting wise to this, and so will prep a victim in advance by contacting them a few days or weeks earlier to change any stored phone numbers or emails to their own. So, it's a good idea to double check any contact when change of details occur. Make sure you double check via the original contact details.

**REMEMBER** – Don't change bank details without double checking.

**CAUTION** – Sometimes, criminals will call in advance to fraudulently change contact numbers. Check when these change too.

**THINK** - Why does this payment have to be made?

### 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](http://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.



**METROPOLITAN  
POLICE**



# Richmond Cyber Crime Summary

## April 2025

- **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**

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](http://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](http://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](mailto: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>



**METROPOLITAN  
POLICE**

