Kensington & Chelsea Fraud Cyber Crime Summary May 2025

Executive Summary

Number of offences	109
Total loss	£734,467.43
Average per victim	£6,738.23

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB52C - Hacking - Social Media and Email	18	£0.00
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	15	£77,424.22
NFIB1H - Other Advance Fee Frauds	11	£18,624.39
NFIB3A - Online Shopping and Auctions	10	£18,243.35
NFIB2E - Other Financial Investment	8	£146,620.00

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

Fraud Type	Amount Lost	Amount of Offences
NFIB19 - Fraud by Abuse of Position of Trust	£306,000.00	1
NFIB2E - Other Financial Investment	£146,620.00	8
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£77,424.22	15
NFIB1E - Fraud Recovery	£60,000.00	1
NFIB2A - Share sales or Boiler Room Fraud	£50,000.00	2

Fraud Advice

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

Kensington & Chelsea Fraud Cyber Crime Summary May 2025

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

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.

Banking and Card Fraud

Bank account fraud has occurred if transactions you haven't made show up on your bank statement.

Bank account fraud could happen as a result of identity theft, when cards or bank account information has been stolen.

How to Protect Yourself

- Don't throw out anything with your name, address or financial details without shredding it first.
- If you receive an unsolicited email or phone call from what appears to be your bank or building society asking for your security details, never reveal your full password, login details or account numbers. Most banks will not approach their customers in this manner.
- If you are concerned about the source of a call, ask the caller to give you a main switchboard number for you to be routed back to them. Alternatively, hang up and call your bank back on the legitimate phone number printed on your bank statements.
- Check your statements carefully and report anything suspicious to the financial institution concerned.
- If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or Credit Card Company.
- Don't leave things like bills lying around for others to look at.
- If you move house, always get Royal Mail to redirect your post.
- Get regular copies of your credit report from a credit reference agency.

Notify your bank immediately if you see any unusual activity on your account.

Kensington & Chelsea Fraud Cyber Crime Summary May 2025

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.
- **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.

Kensington & Chelsea Fraud Cyber Crime Summary May 2025

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

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