

Kensington & Chelsea Fraud Cyber Crime Summary

February 2025

Executive Summary

Number of offences	83
Total loss	£619,448.82
Average per victim	£7,463.24

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	12	£327,114.54
NFIB3D - Other Consumer Non Investment Fraud	11	£77,456.49
NFIB1H - Other Advance Fee Frauds	9	£3,433.18
NFIB3A - Online Shopping and Auctions	9	£4,397.45
NFIB2E - Other Financial Investment	5	£39,447.87

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

Fraud Type	Amount Lost	Amount of Offences
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)	£327,114.54	12
NFIB3C - Door to Door Sales and Bogus Tradesmen	£119,650.00	3
NFIB3D - Other Consumer Non Investment Fraud	£77,456.49	11
NFIB2E - Other Financial Investment	£39,447.87	5
Push Payment	£29,344.68	3

Fraud Advice

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.

Kensington & Chelsea Fraud Cyber Crime Summary

February 2025

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.

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.

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

Kensington & Chelsea Fraud Cyber Crime Summary

February 2025

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?

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.

Kensington & Chelsea Fraud Cyber Crime Summary

February 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 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>