Anti - Fraud Guidelines

In recent years, telecom fraud has become increasingly sophisticated, with frequent scam cases in the UK targeting Chinese students and residents.

During peak business periods, such as the start of the academic year, scammers take advantage of the increased demand for SIM card purchases and international communication services. Many fraudsters spoof phone numbers to impersonate 10086 or other official customer service numbers to carry out scams. They exploit students' unfamiliarity with their new environment, setting up elaborate schemes to steal their money. Additionally, through step-by-step manipulation, scammers not only obtain personal information but also collect facial and voice data via video calls.

CMLink would like to clarify the following:

- CMLink customer service representatives will never ask for your bank card details or request any private identification information over the phone.
- CMLink customer service representatives will never direct customers to other chat apps (e.g., WeChat, WhatsApp, Signal) or transfer calls to alleged police or other "official" institutions.
- CMLink does not require personal identity verification, as UK CMLink SIM cards are non-real-name registered. Therefore, general customer service inquiries do not involve verifying personal details.

The official 10086 customer service team will not proactively call users. CMLink will only contact customers regarding SIM card usage or logistics issues based on customer inquiries.

If you receive a suspicious call from +86 (10) 086 or any other questionable number claiming to be from CMLink, please hang up immediately and call 10086 to verify.

As a UK-based virtual mobile network operator, CMLink is committed to providing convenient telecom services while prioritizing the protection of users' financial security and personal privacy. We strictly adhere to UK regulations and GDPR (General Data Protection Regulation). To safeguard our users, we regularly issue fraud prevention alerts via various channels.

<u>Common Fraud Tactics</u>

Fraudsters often impersonate government officials and use the following deceptive methods:

1. Impersonation of Government Officials

Scammers disguise their caller ID as the Chinese Embassy in the UK, domestic police departments, or other official agencies. They may possess personal details (name, address, identity number) obtained through illegal means, making their deception more convincing.

2. False Allegations of Criminal Involvement

Scammers claim that the victim’s bank account, SIM card, ID card, or medical insurance card has been used for illegal activities. They may instruct victims to visit the embassy to collect documents or allege that they are involved in money laundering, illegal immigration, or drug trafficking.

3. Fake Law Enforcement Actions

Fraudsters pretend to be law enforcement officers, falsely stating that the victim is wanted by the Chinese police. They use chat apps like WeChat or WhatsApp to send fake arrest warrants,

confidentiality agreements, or police credentials. To increase credibility, scammers threaten victims with arrest warrants or extradition. Forbid victims from using the internet or contacting family and friends. Demand regular location check-ins until they succeed in extorting money.

4. Fraudulent Requests for Money Transfers

Victims are tricked into believing they must "prove their innocence" by transferring funds into a so-called "safe account", which is controlled by the scammer.

5. Fake Parcel Delivery Scams

Scammers pose as courier companies, claiming there are issues with a package. They send fake refund links that closely resemble official websites, tricking victims into entering sensitive financial details. Some scam calls even originate from +44 UK-based numbers to appear more credible.

6. AI-Generated Voice Scams

Fraudsters use AI to clone voices and impersonate victims or their relatives, contacting family members in China and fabricating emergencies to solicit money transfers.

How to Protect Yourself

1. Embassies or government agencies will never call you to notify you of criminal involvement.
2. Official institutions will not send sensitive documents via app platforms.
3. Never provide personal banking details or transfer money to unknown accounts.
4. Be cautious of suspicious calls. Do not share personal information, bank details, or click on unknown links. Hang up immediately to avoid financial loss.
5. Use your phone's call-blocking feature to filter out suspicious numbers. You can also forward phishing or spam messages to 7726.
6. If you become a victim of fraud, immediately contact the UK police by calling 999 or reporting it via Action Fraud. Alternatively, call 0300 123 2040 for fraud assistance.
7. If the scam involved a transfer via a Chinese bank, report it to the local Chinese police department or ask a family member in China to immediately call 96110 or 110 (China's anti-fraud hotline).

Important Contact Numbers

Save the following emergency numbers for verification or assistance:

UK Emergency Services: Call 999 (for non-emergencies, dial 101) or visit Action Fraud.

Chinese Ministry of Foreign Affairs Global Consular Protection Hotline:

+86-10-12308 or +86-10-65612308

Chinese Embassy in the UK: +44-7810792326

Chinese Consulate in Manchester: +44-161-2248986

Chinese Consulate in Edinburgh: +44-131-3374449

Chinese Consulate in Belfast: +44-7895306461

If you need to discuss this issue further, please contact us via our hotline or email. Details are as follows:

CMLink users in the UK/EU: 10086

CMLink users in China: +44 7973 000186

Non-CMLink users: +44 7973 000186 (charges may apply, check with your provider)

Email address: csuk@cmlink.com

How to Report Fraud in the UK

Telephone Preference Service (TPS)

Call: 0845 070 0707

Online Report: TPS Complaints

Mail: Telephone Preference Service (TPS), DMA House, 70 Margaret Street, London W1W 8SS

Information Commissioner's Office (ICO)

Call: 0303 123 1113

Online Report: ICO Complaints

Mail: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Ofcom (UK Communications Regulator)

Call: 0300 123 3333

Online Report: Ofcom Complaints

Mail: Ofcom, Riverside House, 2a Southwark Bridge Road, London, SE1 9HA