Beware of "Guess Who" Scams: Stay Alert to Any Request for Money Transfers, No Matter How Familiar the Caller Sounds!

The Police have recently received multiple reports of "Guess Who" scams, showing an upward trend. Elderly victims have suffered losses ranging from several thousand to tens of thousands of dollars. Many elderly individuals, with limited exposure to anti-scam information, believe callers simply because the voices sound familiar.

The Anti-Deception Coordination Centre would like to remind members of the public:

- When receiving urgent requests for money transfers, verify the caller's identity regardless of familiarity or voice similarity. Confirm by calling back directly or meeting in person.
- Scammers often collect your personal and family information in advance, then impersonate acquaintances to make their approach more convincing.
- Be highly cautious if asked to transfer money to unfamiliar bank accounts.
- For elderly persons without online banking, scammers may suggest that a "friend" or "lawyer" collect cash on their behalf. Do not comply.
- Always stay calm and verify any request involving money. Never rush into making transfers.
- Show care for elderly acquaintances and share anti-scam information regularly.
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

Three Common Scam Tactics:

(1) Scripted Approach

1. After illegally obtaining personal data, scammers fabricate identities, invent excuses for transfers, and may even mimic voices.
2. They contact victims via phone/messaging apps to request money transfers.

(2) Account Takeover

1. Scammers hijack victims' messaging accounts and review chat histories to learn about contacts and relationships.
2. They then request money transfers from the victim's contacts via the compromised account.

(3) Cold Call Deception

1. Scammers make casual phone calls without revealing their identity, tricking victims into guessing who they are.
2. Once the victim makes a guess, the scammer immediately assumes that identity.

Recent Cases:

(1) A 62-year-old retiree received a call from a scammer posing as "a staff member of a law firm", claiming that the victim's husband had been involved in a traffic accident last year (the accident was genuine, and the scammer had unlawfully obtained the victim's personal data). The scammer stated that compensation matters were being handled and demanded an upfront "handling fee" of HK$20,000. The victim

transferred the money without verification and was defrauded.

(2) An 86-year-old elderly person received a call from a scammer claiming to be her "daughter" who had recently changed her phone number. Due to the similar voice, the victim did not suspect anything. The following day, the scammer called again, claiming to be short of money and asked the victim to bring cash to a designated housing estate for collection. The victim complied and met a middle-aged man who claimed to be collecting money on behalf of the "daughter." After calling the scammer to confirm, the victim handed over the cash and was defrauded, losing approximately HK$35,000.

(3) A 69-year-old engineer received a WhatsApp message from someone claiming to be his "cousin", stating an urgent need for HK$12,000 and promising repayment in two days. As the victim was busy with work, he transferred the money to an unfamiliar bank account without further verification. The scammer later requested an additional HK$80,000. The victim became suspicious and attempted to call his cousin via WhatsApp, but there was no answer. The scammer then sent a voice message urging the transfer again. Fortunately, the victim remained alert and contacted his cousin directly by phone, discovering that the WhatsApp account had been hacked.

(4) A scammer imitated the voice of an 83-year-old retiree's "nephew" and claimed to have been detained by the police, urgently requesting HK$10,000 for bail. Believing the voice to be genuine, the victim followed instructions to scan an Alipay QR code at a convenience store to make the transfer. Later that day, the victim contacted his niece and discovered it was a scam, resulting in a loss of approximately HK$6,000.

(5) A scammer posing as a telecommunications company customer service officer called a 66-year-old restaurant worker, falsely claiming that the victim owed HK$250 and would face a penalty of HK$5,000 if not paid immediately. Believing the claim to be true, the victim followed instructions to transfer money via an ATM while remaining on the call throughout. After transferring HK$10,000, the scammer demanded a further HK$50,000. The victim became suspicious and promptly reported the case to the police.