集友銀行
Chiyu Banking Corporation Ltd.

Dear Valued Customer,

“AlipayHK YAS” Unauthorised Deduction Scams! Man Transferred $150,000 in a Hurry

Recently, there were a number of scams involving scammers posing as AlipayHK or its insurance partner YAS! The scammers claimed that victims had “accidentally” ticked or automatically activated YAS protection on their AlipayHK apps. They said that free trials had been offered at first, but such protection was about to expire or would be upgraded to paid service soon. If the victims did not cancel the service, fees would be automatically deducted from their accounts every month, or one-off payments of thousands of dollars would be deducted!

Some scammers even fabricated insurance policies to make the scams more realistic. Following instructions in a hurry, a member of the public was cheated out of almost $150,000.

YAS has issued a statement to remind members of the public of scams involving scammers posing as YAS. It emphasises that:

- YAS will never proactively ask its customers for any personal or payment information, including (but not limited to) identity card numbers, banking or credit card information, AlipayHK or other payment account information, and one-time passwords (OTPs);
- YAS will never ask its customers to cancel insurance policies, make refunds or carry out emergency operations via external links, messages or phone calls;
- Any messages claiming “that instant verification is required”, “cancellation of insurance policies” or “refunds”, and asking for information highly likely involve scams;
- Members of the public should make enquiries about their insurance policies or get service via YAS official app, official website or formal customer service channels only.

I. Defrauding Tricks

- Scammers send phishing SMSs, make phone calls or send messages on WhatsApp, claiming that they are AlipayHK or YAS staff members. Being able to mention information such as names or phone numbers, they claim that fees for YAS protection service will be deducted soon and that autopay will be arranged if such service is not cancelled in time.

- Ask victims to call another "cancellation helpline" or contact another WhatsApp account.

- Provide fraudulent URLs to ask victims for personal information, bank account numbers, OTPs, etc.; or show counterfeit insurance policies, threatening to "lock accounts or deduct credits if complete information is not provided".

- Lure victims to transfer money to designated accounts on the pretext of "handling fee", "verification fee", "unlocking fee", etc.

Real Case One

A man received an unsolicited phone call. Mentioning the victim's name correctly, the caller claimed that they were an AlipayHK staff member and that he had "accidentally" ticked YAS protection when opening his account. The protection was on a free trial at first, but had been upgraded to paid service, so a premium of $40,000 would be automatically deducted from his bank account every year!

Upon hearing this message, the victim was frightened and called another "cancellation helpline" according to instructions. Claiming that they were an insurance company staff member, the scammer lured him to visit a fraudulent website to fill in personal information, bank account numbers, credit card information, etc. The scammer even said that if he did not want the deduction, he must submit complete banking information for verification, otherwise their system would lock his bank accounts immediately!

Being extremely anxious, the victim made a transfer in a hurry, so was cheated out of almost $150,000. He only knew that the whole process was just a scam after making a report to the police.

Real Case Two

A victim received a phone call whose caller claimed that they were a "YAS Insurance" staff member. The caller said that an insurance policy of the victim was about to expire and asked if the victim wanted to renew it. The victim said that such policy had never been bought, and then the caller changed their tune immediately, saying that they would help the victim make a cancellation to avoid the deduction.

By luring the victim to log on to a fraudulent website, the fake staff member asked the victim to transfer a "verification fee" of over $30,000, and promised that it would be refunded in full later in the day. The victim became more and more suspicious of the transfer after making it, so made a report to the police, but the amount had been lost.

II. Police Advice

- Do not call phone numbers in SMSs or click on unknown hyperlinks;
- Do not share your screen with strangers;
- Do not hastily click on hyperlinks, download mobile applications, log on to any suspicious websites or download any attachments;
- You may enter suspicious phone numbers, URLs or transferees' account numbers on "Scameter" of CyberDefender or "Scameter+", the mobile application of "Scameter", for security check in addition to seeking verification from relevant organizations;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

Please refer to the following website for the Police anti-deception information：
https://www.adcc.gov.hk/en-hk/alerts.html

Chiyu Banking Corporation Limited

July 2026