Scam prevention alert in FPS payment

Q1: If I find my recipient's FPS proxy ID is being flagged by the scam prevention alert, how can I remove it?

The scam prevention alert is generated based on information collected from scam reports and recorded in the Scameter of the Hong Kong Police Force. Please contact them at enquiry@cyberdefender.hk if you think the FPS proxy IDs are not tagged correctly.

Q2: Will Bank be able to help to remove my FPS proxy IDs from the scam prevention alert?

No, the Bank cannot do the deletion. The scam prevention alert is generated based on information collected from scam reports and recorded in the Scameter of the Hong Kong Police Force. Please contact them at enquiry@cyberdefender.hk if you think the FPS proxy IDs are not tagged correctly.

Q3: If I want to report a suspicious FPS proxy ID, what should I do?

The scam prevention alert is generated based on information collected from scam reports and recorded in the Scameter of the Hong Kong Police Force. If you suspect a crime case has occurred, please report to the Hong Kong Police Force at a police station or via Hong Kong Police Force e-Report Centre (https://www.police.gov.hk/ppp_en or https://www.police.gov.hk/ppp_tc).

Q4: If there is no scam prevention alert message relating to my recipient, does it guarantee it is safe to transfer to him/her?

No, it is not guaranteed. The scam prevention alert message will only be shown if the recipient's FPS proxy ID is included in the scam reports provided by the Hong Kong Police Force. If there has not been any report to the Police against a particular FPS proxy ID, the proxy ID will not be included in the scam prevention alert.

You are advised to always verify the payment details (including the recipient's identity) of every single transaction before making payment.

Q5: Why is my recipient's FPS proxy ID previously not tagged in the scam prevention alert but now being tagged?

The FPS proxy IDs flagged as "High Risk" in Scameter and included in the scam prevention alert are based on information collected from scam reports provided by the Hong Kong Police Force. If there has not been any report to the Police against a particular FPS proxy ID, the proxy ID will not be included in the scam prevention alert.

Q6: What is the source of the scam prevention alert and how is my private information being protected?

The scam prevention alert is generated based on information collected from scam reports and recorded in the Scameter of the Hong Kong Police Force. Please visit the webpage of Scameter (https://cyberdefender.hk/en-us/scameter/) for more details.

Q7: Why I found my FPS proxy ID on the scam prevention alert when doing FPS transfer? I did not commit any crime!

According to the record provided by the Hong Kong Police Force, your FPS proxy ID is related to a scam report. Please contact them at enquiry@cyberdefender.hk if you think the FPS proxy ID is not tagged correctly.

Q8: I discovered my recipient's mobile number has been flagged in Scameter. How come the bank did not alert me when I **now** try to make payment to this FPS proxy ID?

The scam prevention alert is generated based on information collected from scam reports provided by the Hong Kong Police Force and updated from time to time on a daily basis. Please check again that the payee is trustworthy before you proceed with the transaction.

Q9: I discovered my recipient's mobile number has been flagged in Scameter. How come the bank did not alert me when I **previously** made payment to this FPS proxy ID?

The FPS proxy IDs flagged as "High Risk" in Scameter and included in the scam prevention alert are based on information collected from scam reports provided by the Hong Kong Police Force. If there has not been any report to the Police against a particular FPS proxy ID, the proxy ID will not be included in the scam prevention alert.

Q10: Why are scam prevention alerts generated only for FPS proxy IDs when I conduct online transfers but no scam prevention alert is generated for bank accounts? (the online Scameter offers search service of suspicious bank accounts too)

The scope of this scam prevention alert mechanism in the first stage covers FPS proxy IDs. The scope will be reviewed from time to time.

Q11: How would I know if my recipient’s mobile number/email address/FPS Identifier is flagged for scam prevention alert?

You can check Scameter (cyberdefender.hk) to see if it is flagged as “High Risk”. When performing an FPS transaction with use of FPS proxy ID (i.e. mobile number, email address, or FPS Identifier) via internet banking or mobile banking app, the Bank will display a scam prevention alert message for those FPS proxy IDs flagged in the scam reports provided by the Hong Kong Police Force. You are advised not

to make any transactions to the recipient unless you have carefully verified the recipient's identity and ensure that the recipient is trustworthy.

Q12: If I confirm to the bank to proceed with an FPS transfer with FPS proxy ID (i.e. mobile number/email address/FPS Identifier) flagged as "High Risk" and subsequently realize being scammed, what should I do?
If you suspect you have been scammed, you may visit a police station or the Hong Kong Police Force e-Report Centre (https://www.police.gov.hk/ppp_en or https://www.police.gov.hk/ppp_tc) to file a report. In tandem, please report the case to the Bank.

Q13: If a recipient's mobile number is flagged as "High Risk", will his/her email address or FPS Identifier also be flagged by the scam prevention alert?
The FPS proxy IDs flagged as "High Risk" in Scameter and included in the scam prevention alert are based on information collected from scam reports provided by the Hong Kong Police Force. If there has not been any report to the Police against a particular FPS proxy ID, the proxy ID will not be included in the scam prevention alert.

Q14: Can I confirm and accept the scam prevention alert message and make FPS transfer to the FPS proxy ID on the scam prevention alert?
Yes, you can, but please be reminded that the transaction has high risk of fraud. You are advised to always verify the payment details (including the recipient's identity) of every single transaction before making payment.