

Questions related to high risk alert

Q1: If I find my payee 's FPS proxy ID / bank account number / SVF account number is being flagged as a high risk alert, how can I remove it?

The high risk 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 / bank account numbers / SVF account numbers are not tagged correctly or if you think there is an error with the information/alert.

Q2: Will Bank / SVF operator be able to help to remove my FPS proxy IDs / bank account numbers / SVF account numbers from the high risk alert?

No, the Bank / SVF operator cannot do the deletion. The high risk 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 / account numbers are not tagged correctly or if you think there is an error with the information/alert.

Q3: If I want to report a suspicious FPS proxy ID / bank account number / SVF account number, what should I do?

The high risk 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 call "Anti-Scam Helpline 18222" hotline for assistance. If you suspect that you have fallen prey to a scam, 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 high risk alert message relating to my payee does it guarantee it is safe to transfer to him/her?

No, it is not guaranteed. The alert message will only be shown if the payee 's FPS proxy ID / bank account number / SVF account number 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 / bank account number / SVF account number, the proxy ID / account number will not be included in the high risk alert.

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

Q5: Why is my payee 's FPS proxy ID / bank account number / SVF account number previously not tagged in the high risk alert but now being tagged?

The FPS proxy IDs / bank account number / SVF account number flagged as "High Risk" in Scameter and included in the high risk 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 / bank account number / SVF account number, the proxy ID / account number will not be included in the high risk alert.

- Q6: What is the source of the high risk alert and how is my private information being protected?
The high risk 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 / bank account number / SVF account number being shown as the high risk alert when doing transfer? I did not commit any crime!
According to the record provided by the Hong Kong Police Force, your FPS proxy ID / bank account number / SVF account number is related to a scam report. Please contact them at enquiry@cyberdefender.hk if you think the FPS proxy ID / bank account number / SVF account number is not tagged correctly.
- Q8: I discovered my payee's mobile number / account number has been flagged in Scameter. How come the bank / SVF operator did not alert me when I **now** try to make payment to this FPS proxy ID / bank account number / SVF account number?
The high risk 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 payee 's mobile number / account number has been flagged in Scameter. How come the bank / SVF operator did not alert me when I **previously** made payment to this FPS proxy ID / bank account number / SVF account number?
The FPS proxy IDs flagged as "High Risk" in Scameter and included in the high risk 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 proxy ID / account number, the proxy ID / account number will not be included in the high risk alert.
- Q10: How would I know if my payee 's mobile number / email address / FPS Identifier / bank account / SVF account is flagged for high risk alert?
You can check Scameter (cyberdefender.hk) to see if it is flagged as "High Risk". When performing a transaction with use of FPS proxy ID (i.e. mobile number, email address, or FPS Identifier) / bank account / SVF account via internet banking / mobile banking app / SVF app/ bank counter/ ATM, the Bank / SVF will display a high risk alert message for those FPS proxy IDs / bank accounts / SVF accounts flagged in the scam reports provided by the Hong Kong Police Force. You are advised not to make any transactions to the payee unless you have carefully verified the payee 's identity and ensure that the payee is trustworthy.

Q11: If I confirm to the bank to proceed with a transfer with FPS proxy ID (i.e. mobile number / email address / FPS Identifier) / bank account / SVF account 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.

Q12: If a payee’s mobile number is flagged as “High Risk”, will his/her email address / FPS Identifier / bank account number / SVF account number also be flagged by the high risk alert?

The FPS proxy IDs / bank account number / SVF account number flagged as "High Risk" in Scameter and included in the high risk 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 / account number, the proxy ID / account number will not be included in the high risk alert.

Q13: Can I confirm and accept the high risk alert message and make transfer to the FPS proxy ID / bank account number / SVF account number on the high risk 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 payee’s identity) of every single transaction before making payment.