1. Q: What is the source of the scam prevention alert and how is my private information being protected?
   A: 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.

2. Q: If I find my recipient's FPS proxy ID (i.e. mobile number, email address, or FPS Identifier) is being flagged by the scam prevention alert, how can I remove it?
   A: 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.

3. Q: Will Bank be able to help to remove my FPS proxy IDs from the scam prevention alert?
   A: 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.

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

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

6. Q: How would I know if my recipient's mobile number/email address/FPS Identifier is flagged for scam prevention alert?
   A: 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 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.

7. Q: If I confirm to proceed with an FPS transfer with FPS proxy ID flagged as "High Risk" and subsequently realize being scammed, what should I do?
   A: 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.

8. Q: 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?
   A: 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.

9. Q: Can I confirm and accept the scam prevention alert message and make FPS transfer to the FPS proxy ID on the scam prevention alert?
   A: 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.

1. 問： 請問「防騙警示」的資料來源是甚麼，以及我的私人資料如何受到保障？
答： 「防騙警示」的資料來自公眾的詐騙舉報並收錄於香港警務處的「防騙視伏器」。如欲了解更多詳情，請瀏覽「防騙視伏器」網頁 (https://cyberdefender.hk/scameter)。

2. 問： 如果我收款人的「轉數快」識別代號（即手機號碼、電郵地址或快速支付系統識別碼）被「防騙警示」標示，我可如何移除標示？
答： 「防騙警示」的資料來自公眾的詐騙舉報並收錄於香港警務處的「防騙視伏器」。如您認為有關標示有誤，請發電郵至 enquiry@cyberdefender.hk 與香港警務處聯絡。

3. 問： 銀行能否協助把我的「轉數快」識別代號從「防騙警示」移除？
答： 本行不能作出移除。「防騙警示」的資料來自公眾的詐騙舉報並收錄於香港警務處的「防騙視伏器」。如您認為有關標示有誤，請發電郵至 enquiry@cyberdefender.hk 與香港警務處聯絡。

4. 問： 如我沒有收到有關收款人的警示訊息，是否就能確保向他/她轉賬是安全的？
答： 不能確保。警示訊息只會在收款人的「轉數快」識別代號在香港警務處提供的「防騙警示」資料中出現時，方會發出。如尚未有公眾向警方舉報有關「轉數快」識別代號，該識別代號將不會在「防騙警示」內。
本行建議您在每次交易付款前均核實付款詳情（包括收款人身份）。

5. 問： 我用「轉數快」轉賬時發現自己的「轉數快」識別代號被「防騙警示」標示。我並無犯罪為何會這樣！
答： 根據香港警務處提供的記錄，您的「轉數快」識別代號與詐騙舉報有關。如您認為有關標示有誤，請發電郵至 enquiry@cyberdefender.hk 與香港警務處聯絡。

6. 問： 我如何得知收款人的手機號碼/電郵地址/快速支付系統識別碼是否已被「防騙警示」標示？
答： 您可以透過「防騙視伏器」（cyberdefender.hk）查看有否被標示為「高危有伏」。當透過網上銀行或流動銀行應用程式使用「轉數快」識別代號進行「轉數快」交易時，如收款人的「轉數快」識別代號在香港警務處提供的「防騙警示」資料上出現，本行會就該等「轉數快」識別代號發出警示。本行建議除非您已小心核實收款人的身份並確保其可靠，否則不要與收款人進行任何交易。

7. 問： 如我確認向被標示為「高危有伏」的「轉數快」識別代號進行「轉數快」轉賬，而其後發現被騙，我該怎辦？
答： 如您懷疑被騙，請到警署或透過電子報案中心(https://www.police.gov.hk/ppp_en 或 https://www.police.gov.hk/ppp_tc) 向香港警務處報案。同時並請向本行舉報。

8. 問： 如收款人的手機號碼被標示為「高危有伏」，他/她的電郵地址或快速支付系統識別碼會否也被「防騙警示」標示？

答： 「防騙視伏器」內標籤為「高危有伏」並列入「防騙警示」的「轉數快」識別代號均來自市民向香港警務處的詐騙舉報。如尚未有公眾向警方舉報有關「轉數快」識別代號，該識別代號將不會在「防騙警示」內。

9. 問： 我可否在確認和接受「防騙警示」訊息後向出現在「防騙警示」上的「轉數快」識別代號的收款人進行「轉數快」轉賬？

答： 可以，但請留意有關轉賬存在高度詐騙風險。本行建議您在每次交易付款前均核實付款詳情（包括收款人身份）。

1. 问： 请问「防骗警示」的数据来源是什么，以及我的私人数据如何受到保障？
答： 防骗警示的资料来自公众的诈骗举报并收录于香港警务处的「防骗视伏器」。 如欲了解更多详情，请浏览「防骗视伏器」网页（https://cyberdefender.hk/scameter）。

2. 问： 如果我收款人的「转数快」识别代号（即手机号码、电邮地址或快速支付系统识别码）被「防骗警示」标示，我可如何移除标示？
答： 「防骗警示」的资料来自公众的诈骗举报并收录于香港警务处的「防骗视伏器」。 如您认为有关标示有误，请发电邮至 enquiry@cyberdefender.hk 与香港警务处联络。

3. 问： 银行能否协助把我的“转数快”识别代号从“防骗警示”移除？
答： 本行不能作出移除。 「防骗警示」的资料来自公众的诈骗举报并收录于香港警务处的「防骗视伏器」。 如您认为有关标示有误，请发电邮至 enquiry@cyberdefender.hk 与香港警务处联络。

4. 问： 如我没有收到有关收款人的警示讯息，是否就能确保向他/她转账是安全的？
答： 不能确保。 警示讯息只会在收款人的「转数快」识别代号在香港警务处提供的「防骗警示」资料中出现时，方会发出。 如尚未有公众向警方举报有关「转数快」识别代号，该识别代号将不会在「防骗警示」内。
本行建议您在每次交易付款前均核实付款详情（包括收款人身份）。

5. 问： 我用「转数快」转账时发现自己的「转数快」识别代号被「防骗警示」标示。 我并无犯罪为何会这样！
答： 根据香港警务处提供的记录，您的「转数快」识别代号与诈骗举报有关。 如您认为有关标示有误，请发电邮至 enquiry@cyberdefender.hk 与香港警务处联络。

6. 问： 我如何得知收款人的手机号码/电邮地址/快速支付系统识别码是否已被「防骗警示」标示？
答： 您可以通过「防骗视伏器」（cyberdefender.hk）查看有否被标示为「高危有伏」。 当透过网上银行或流动银行应用程序使用「转数快」识别代号进行「转数快」交易时，如收款人的「转数快」识别代号在香港警务处提供的「防骗警示」资料上出现，本行会就该等「转数快」识别代号发出警示。 本行建议除非您已小心核实收款人的身份并确保其可靠，否则不要与收款人进行任何交易。

7. 问： 如我确认向被标示为“高危有伏”的「转数快」识别代号进行「转数快」转账，而其后发现被骗，我该怎办？
答： 如您怀疑被骗，请到警署或透过电子报案中心（https://www.police.gov.hk/ppp_en 或 https://www.police.gov.hk/ppp_tc）向香港警务处报案。 同时并请向本行举报。

8. 问： 如收款人的手机号码被标示为「高危有伏」，他/她的电邮地址或快速支付系统识别码会否也被「防骗警示」标示？

答： 「防骗视伏器」内标签为「高危有伏」并列入「防骗警示」的「转数快」识别代号均来自市民向香港警务处的诈骗举报。 如尚未有公众向警方举报有关「转数快」识别代号，该识别代号将不会在「防骗警示」内。

9. 问： 我可否在确认和接受“防骗警示”消息后向出现在“防骗警示”上的「转数快」识别代号的收款人进行「转数快」转账？

答： 可以，但请留意有关转账存在高度诈骗风险。 本行建议您在每次交易付款前均核实付款详情（包括收款人身份）。