

使用網上交易/流動支付服務的保安提示

(Q1 及 Q2 適用於信用卡/多幣扣賬卡持卡人)

1. 持卡人有甚麼網上交易的保安資訊要注意？

- 若進行網上交易前，請確保網上購物平台安全可靠，並時刻對不明網址保持警惕以免墜入欺詐陷阱，例如「釣魚短訊」。未確定平台或網址真實性前，切勿透露任何個人資料、銀行帳號或信用卡/多幣扣賬卡資料，如網上銀行登入密碼、進行轉帳交易或透過超連結登入可疑網頁。
- 你需清楚核對手機短訊或 inMotion 動感銀行上顯示之交易內容及細節，如商戶名稱、交易種類、交易金額或貨幣等是與你的交易相同後才輸入一次性密碼或使用 inMotion 動感銀行認證以完成網上交易。請保障交易內容及細節安全和保密。
- 時刻留意本行(包括主頁底部的「網上保安」連結)、香港警務處(包括其網頁內的防止罪案建議及「反詐騙協調中心」的騙案警示)、監管機構、政府部門或其他機構等之保安資訊。
- 如你持續發現有任何可疑交易，可要求本行對商戶停止有關交易。你的交易受退款保障機制保障，適用範圍包括經一次性密碼或 inMotion 動感銀行驗證之爭議交易，如你對交易有懷疑，本行會按交易組織機構的保障機制及規則協助你作出相關調查及跟進。如屬信用卡交易及你在到期付款日前向本行作出未經授權交易的報告，你有權在調查期間拒絕支付涉及爭議的款額。
- 請確保閣下登記用於接收本行重要通知的聯絡方式是最新的，並留意本行的通知。
- 避免使用不加密或不明的公眾 WIFI 處理敏感資料活動，包括使用信用卡/多幣扣賬卡網上購物。
- 如商戶英文名稱從缺，本行的通知可能使用「商戶」代替。

2. 如果我的信用卡/多幣扣賬卡或認證因素遺失、被盜用，或認證因素或卡資料已遭泄露，應如何處理？

請立即致電信用卡/多幣扣賬卡報失熱線(852) 3603 7899 以作安排。如發現異常、可疑或未經授權交易，你亦應立即經同一熱線、inMotion 動感銀行或網上理財向本行報告。

(Q3 至 Q14 適用於信用卡持卡人)

3. 流動支付交易安全嗎？

流動支付是一個安全的付款方式。Apple Pay/Google Pay 會以一組獨特的裝置賬戶號碼作為付款資料，你的真正信用卡賬戶號碼及姓名並不會與商戶分享。

4. 什麼卡資料會被儲存於流動裝置內？

Apple Pay

在你加入你的信用卡至 Apple Pay 時，你的實際卡號不會被儲存，你會獲分配一個獨特的裝置賬戶號碼，這個號碼會被加密，並安全地儲進 iPhone、iPad 和 Apple Watch 的專用晶片

Secure Element 上。在你進行購物交易時，便會以這個裝置賬戶號碼及該次交易特定的動態保安編碼來處理付款。因此，Apple 不會向商戶披露你的實際信用卡號碼，而付款時也不必傳送這些資料。

Google Pay

虛擬賬戶號碼是唯一被儲存於流動裝置上的資料，會經由 Google Pay 傳送作為付款交易處理。虛擬賬戶號碼能代表信用卡賬戶而又有別於真正信用卡賬戶號碼，因此能更保障你的賬戶資料。

5. 除了我之外，有沒有人可以使用我的 Apple Pay/Google Pay 付款？

每個擁有你流動裝置密碼或已在流動裝置中登記指紋/Face ID/其他生物辨識憑證(如適用)的人都可以透過 Apple Pay/Google Pay 使用你的信用卡進行認可的交易。你必須保障你的流動裝置安全及你的流動裝置密碼保密。不要讓任何人在你已登記信用卡的設備中儲存他們的指紋/Face ID/其他生物辨識憑證。請經常保持你的流動裝置在上鎖狀態，以避免第三者使用你的流動裝置進行 Apple Pay/Google Pay 交易。避免使用容易取得的個人資料(例如電話號碼、出生日期)或簡單密碼(例如123456)作為密碼。你不應以相同的密碼接駁其他服務，包括連連互聯網或其他網址。

6. 如果我的裝置遺失或被盜，應如何處理？

你可致電信用卡報失熱線(852) 3603 7899 要求暫時停用已儲存於流動裝置上的虛擬賬戶，而你的實體信用卡並不會受影響。你亦可參考本提示 Q14 於 Apple 及 Google 網頁查詢不時更新的裝置遺失或被盜常見問題及解決方案。

7. 如收到續期卡，是否需要更新於 Apple Pay/Google Pay 內的信用卡？

需要。如你之前已於 Apple Pay/Google Pay 登記你的信用卡，當你確認已到期更新的信用卡時，須重新加入該信用卡。於重新加入你的續期卡前請先移除原先已加入 Apple Pay/Google Pay 的舊信用卡。

8. 如收到相同信用卡賬戶號碼之補發卡，我需要於 Apple Pay/Google Pay 之流動裝置中進行更新嗎？

不需要。如果你收到補發信用卡並有同樣的信用卡賬戶號碼、到期日及保安編碼，你的流動裝置將會自動連接到補發卡之信用卡賬戶號碼。當你收到新的信用卡及確認信用卡後，便可繼續使用 Apple Pay/Google Pay 進行交易。

9. 如收到不相同信用卡賬戶號碼之補發卡，我需要於 Apple Pay/Google Pay 之流動裝置中進行更新嗎？

需要。如果你收到補發信用卡而信用卡賬戶號碼或到期日或保安編碼是不相同，你的流動裝置是不會自動連接到補發卡之信用卡賬戶號碼。當你收到新的信用卡及確認信用卡後，需要於 Apple Pay/Google Pay 流動裝置中進行更新，重新將信用卡加至 Apple Pay/Google Pay 才可進行交易。於重新加入你的續期卡前請先移除原先已加入 Apple Pay/Google Pay 的舊信用卡。

10. 如我重設或更新我的流動裝置，會發生什麼事？

當你進行資料重設或更新，所有儲存在 Apple Pay/Google Pay 中的付款資訊將會被移除。你需要在流動裝置重設後，重新設定並加入信用卡至 Apple Pay/Google Pay。

11. 如我更換了我的裝置，應如何處理？

如你更換你的裝置，包括到新型號，那你需要重新加入你的信用卡至 Apple Pay/Google Pay。請緊記在你的裝置買賣、轉讓或丟棄前，把你的信用卡從裝置上移除。

12. 如我需要維修、出售、轉讓或不再使用流動裝置，應怎樣處理？

請確保你於維修、出售或不再使用前已經將流動裝置上所有信用卡資料移除。及後可於流動裝置上重新加入信用卡以繼續使用 Apple Pay/Google Pay 應用程式。

13. 我該如何確保流動裝置及 Apple Pay/Google Pay 的使用安全？

Apple Pay

使用 Face ID 來驗證你的 Apple Pay 交易的建議：

- 請不要從裝置設定中停用「使用 Face ID 需要注視螢幕」功能。如果在任何情況下你需要停用此功能，請不要於 Apple Pay 上使用 Face ID；
- 如你有雙胞胎或樣貌相近的兄弟姐妹，你的兄弟姐妹或可以 Face ID 登入你的 Apple Pay，因此本行建議你不要於 Apple Pay 上使用 Face ID；及
- 如你尚在發育階段或你的臉部特徵可能有所變化，你或不能以 Face ID 登入 Apple Pay，因此本行建議你不要於 Apple Pay 上使用 Face ID。

如你對於 Face ID 的保安存有疑慮，你可使用裝置密碼來驗證你的 Apple Pay 交易。請於「設定」>「Face ID 與密碼」>「使用 Face ID」上關掉「Apple Pay」選項。

Apple Pay/Google Pay

無論你使用那一個型號的裝置，請參考下列貼士以保護你的流動信用卡：

- 設定鎖機密碼 - 建議切勿以令人容易猜測得到的個人資料作為鎖機密碼。
- 請確保所有應用程式從可信的來源下載。
- 切勿瀏覽或點擊可疑網站或網址連結。
- 當不需要使用時，關閉 NFC 功能(如適用)。
- 更新流動裝置的作業系統至最新版本。
- 切勿使用 Jailbreak(越獄)或 Root 機等手法改裝你的裝置。
- 請設定時間較短的螢幕自動關閉功能，以防別人盜用流動支付功能。
- 請時常小心看管你的流動裝置。

14. 如有其他問題，應如何處理？

有關 Apple Pay 請前往“<https://getsupport.apple.com/>”、有關 Google Pay 請前往“support.google.com/googlepay”或致電信銀國際信用卡客戶服務熱線(852) 2280 1288 以查詢信用卡安全、投訴、保安事件或更多資訊。

本通知中英文版本有任何歧義，概以英文版為準。

2025年9月

Security Advice of Online Transaction / Mobile Payment Usage

(Q1 & Q2 are applicable to credit card / multi-currency debit card cardholders)

1. What security tips on online transactions should cardholders be aware of?

- Before conducting online transactions, ensure the shopping sites are secure and authentic. Stay vigilant to unknown hyperlinks to avoid fraud and scams, such as phishing SMS. Never disclose any personal information, bank account numbers or credit card / multi-currency debit card details such as online banking login credentials, transfer money or access suspicious websites unless you confirm the platform or website is authentic.
- Please be reminded to verify the transaction contents and details displayed on your SMS or inMotion, for example, merchant name, transaction type, transaction amount and currency, etc. are all same with your intended transaction before entering the one time password (OTP) or using inMotion authentication to complete the transaction. Keep the transaction contents and details secure and secret to yourself.
- Stay vigilant to the security tips and notice of incidents provided by the Bank (including the link to 'Online Security' at the bottom of our bank website homepage), Hong Kong Police Force (including Crime Prevention advice at the website and scam alerts at Anti-Deception Coordination Centre), regulatory bodies, Government Departments and other relevant organisations.
- You can request the Bank to stop payment to the merchant if you subsequently find yourself to be the victims of phishing scams. Your card transactions under dispute are subject to the protection from chargeback mechanism and the protection is applicable to transactions which have been authorized by OTP or inMotion. The Bank will base on the chargeback mechanism and rules from card associations to assist in investigating any transactions that are in doubt. Where you report an unauthorized credit card transaction before the payment due date, you have the right to withhold payment of the disputed amount during the investigation period.
- Ensure your contact details registered with the Bank are up-to-date to allow relevant important notifications to be delivered to you on a timely basis. Stay vigilant to the notifications from the Bank.
- Do not use unsecured or unknown public WIFI to process sensitive data related activities, including online shopping with credit cards/multi-currency debit cards.
- For merchants without English name, the notification by the Bank may use "a merchant" to represent.

2. What if my credit card / multi-currency debit card or authentication factors have been lost, stolen or the authentication factors or the card information has been compromised?

You should call our Credit Card / Multi-Currency Debit Card Lost Card Reporting Hotline (852) 3603 7899 for arrangement immediately. If you identify unusual, suspicious or unauthorised transactions on your credit card / multi-currency debit card, you should also report to the Bank immediately via the same hotline, inMotion or i-banking.

(Q3 to Q14 are applicable to credit cardholders)

3. Is mobile payment secure?

Mobile payment is a secure way to make payments. A unique Device Account Number will be created to represent your account information by Apple Pay / Google Pay. They do not send your actual

credit card number, name with your payment in the app and will not share with the merchant.

4. What card data is stored on the device?

Apple Pay

When you added your credit card to Apple Pay, instead of using your actual card numbers, a unique Device Account Number is assigned, encrypted, and securely stored in a dedicated chip [Secure Element] in iPhone, iPad and Apple Watch. When you make a purchase, the Device Account Number, along with a transaction-specific dynamic security code, is used to process your payment so your actual card numbers are not shared by Apple with merchants or transmitted with payment.

Google Pay

The only card data stored on a cardmember's mobile device is the "Token" Google Pay passes to the payment processor. This Token represents a cardmember's card and helps to ensure account security because it differs from the credit card number it represents.

5. Can anyone other than me able to use my device for payment?

Anyone with your device "Passcode" or a fingerprint or a Face ID or other biometric authentications (if applicable) registered to your device will be able to authorize transactions using your credit card with Apple Pay/Google Pay. You MUST keep your device safe and secure, and your device "Passcode" secret. Do not let anyone else to have their fingerprint/Face ID/other biometric authentications registered to your device while your credit card is registered with it. Always keeps the mobile device on lock to avoid anyone using your mobile device for payment. It is not suitable to use easily accessible personal information such as telephone numbers or date of birth, or simple password (e.g. 123456) as passcode. You should not use the same passcode for accessing other services, including connection to the internet or accessing other websites.

6. What should I do if my device is lost or stolen?

You can call our Credit Card Lost Card Reporting Hotline (852) 3603 7899 immediately to suspend the virtual account on your device, while your physical credit card is affected. You can also take reference from Q14 of this Advice to check the FAQ and solutions for lost or stolen device updated from time-to-time at Apple and Google websites.

7. If I receive a renewal card, do I need to update the card information in Apple Pay / Google Pay?

Yes. If a card you have previously registered on Apple Pay / Google Pay is renewed, you need to register the Apple Pay / Google Pay with your new card again. Before you do the provisioning again, you need to remove the old card from the Apple Pay / Google Pay first.

8. If I receive a replacement card with the same card number, do I need to update my credit card information with Apple Pay / Google Pay on my existing device?

No. If you receive a replacement card with the same card number, expiry date and security code, your mobile device will connect to your replacement card automatically. You can continue to use your card in Apple Pay / Google Pay to make transactions when you receive and activate your replacement card.

9. If I receive a replacement card with the different card number, do I need to update my credit card information with Apple Pay / Google Pay on my existing device?

Yes. If you receive a replacement card with the different card number or expiry date or security code, your mobile device will not connect to your replacement card automatically. You need to activate your replacement card and register the Apple Pay / Google Pay with your new card again, so that you can continue to use your card in Apple Pay / Google Pay to make transactions. Before you register your new card to Apple Pay / Google Pay again, you may need to remove the old provisioned credit card from the Apple Pay / Google Pay.

10. What happens when I reset, format, or update my device?

When performing a factory data reset, format, or update, all payment information in Apple Pay / Google Pay will be deleted. You will need to set up and enter your credit card(s) information into Apple Pay / Google Pay again after your device has been reset.

11. What happens when I change my device?

If you change your device, including to a new device model, you will need to add your credit card(s) to Apple Pay / Google Pay again. Please ensure that you remove your card(s) from any device before selling, exchanging, or disposing of them.

12. If I have to repair, sell, exchange or no longer use my device, what should I do?

Please make sure to remove all your credit card(s) information from Apple Pay / Google Pay before repairing, selling or stop using your device. And set up Apple Pay / Google Pay and add your credit card again afterward.

13. What can I do to keep my device and card registered with Apple Pay / Google Pay security protected?

Apple Pay

The recommendation of using Face ID to authorize Apple Pay transaction:

- DO NOT disable the "Require Attention for Face ID" function in your device settings. If it has been disabled, do not use Face ID for Apple Pay;
- It is not recommended to use Face ID for Apple Pay if you have a twin sibling or siblings who look very alike as your siblings may be able to logon to your Apple Pay using Face ID; and
- It is not recommended to use Face ID for Apple Pay if you are in puberty stage or your facial features may be undergoing a rapid stage of development as you may not be able to logon to Apple Pay using Face ID.

If you have concern on the security of Face ID, you can use your device Passcode for Apple Pay instead. Please go to "Settings" > "Face ID & Passcode" > "Use Face ID" to turn off the "Apple Pay" option.

Apple Pay / Google Pay

Regardless of your phone model, please be reminded of the following tips to ensure the protection in using your mobile credit card:

- Set a screen lock – do not choose any personal identification number as password that is easy to guess by any other person.
- Make sure all apps are downloaded from trusted sources.
- Do not visit any suspected website and click suspected hyperlinks.
- Turn off NFC when not in use (if applicable).
- Keep the operating system of your device up-to-date.
- Do not modify your device by using methods such as jailbreaking or rooting.
- Set the screen to automatically turn off for a shorter period of time to prevent others from using your mobile payment.
- Always exercise caution in safeguarding your mobile device.

14. What should I do if I encounter other problems?

Please go to "https://getsupport.apple.com/" for Apple Pay or "support.google.com/googlepay" for Google Pay or call our CNCBI Credit Card Customer Service Hotline (852) 2280 1288 for card security enquiries, complaint, security incidents or more information.

If there is any discrepancy between the English and Chinese versions of this Notice, the English version shall prevail.

September 2025

使用网上交易/流动支付服务的保安提示

(Q1 及 Q2 适用于信用卡/多币借记卡持卡人)

1. 持卡人有甚么网上交易的保安资讯要注意？

- 若进行网上交易前，请确保网上购物平台安全可靠，并时刻对不明网址保持警惕以免坠入欺诈陷阱，例如「钓鱼短讯」。未确定平台或网址真实性前，切勿透露任何个人资料、银行帐号或信用卡/多币借记卡资料，如网上银行登入密码、进行转帐交易或透过超连结登入可疑网页。
- 你需清楚核对手机短讯或 inMotion 动感银行上显示之交易内容及细节，如商户名称、交易种类、交易金额或货币等是与你的交易相同后才输入一次性密码或使用 inMotion 动感银行认证以完成网上交易。请保障交易内容及细节安全和保密。
- 时刻留意本行(包括主页底部的「网上保安」连结)、香港警务处(包括其网页内的防止罪案建议及「反诈骗协调中心」的骗案警示)、监管机构、政府部门或其他机构等之保安资讯。
- 如你持续发现有任何可疑交易，可要求本行对商户停止有关交易。你的交易受退款保障机制保障，适用范围包括经一次性密码或 inMotion 动感银行验证之争议交易，如你对交易有怀疑，本行会按交易组织机构的保障机制及规则协助你作出相关调查及跟进。如属信用卡交易及你在到期付款日前向本行作出未经授权交易的报告，你有权在调查期间拒绝支付涉及争议的款额。
- 请确保阁下登记用于接收本行重要通知的联络方式是最新的，并留意本行的通知。
- 避免使用不加密或不明的公众 WIFI 处理敏感资料活动，包括使用信用卡/多币借记卡网上购物。
- 如商户英文名称从缺，本行的通知可能使用「商户」代替。

2. 如果我的信用卡/多币借记卡或认证因素遗失、被盗用，或认证因素或卡资料已遭泄露，应如何处理？

请立即致电信用卡/多币借记卡报失热线(852) 3603 7899 以作安排。如发现异常、可疑或未经授权交易，你亦应立即经同一热线、inMotion 动感银行或网上理财向本行报告。

(Q3 至 Q14 适用于信用卡持卡人)

3. 流动支付交易安全吗？

流动支付是一个安全的付款方式。Apple Pay/Google Pay 会以一组独特的装置账户号码作为付款资料，你的真正信用卡账户号码及姓名并不会与商户分享。

4. 什么卡资料会被储存于流动装置内？

Apple Pay

在你加入你的信用卡至 Apple Pay 时，你的实际卡号不会被储存，你会获分配一个独特的装置账户号码，这个号码会被加密，并安全地储进 iPhone、iPad 和 Apple Watch 的专用晶片

Secure Element 上。在你进行购物交易时，便会以这个装置账户号码及该次交易特定的动态保安编码来处理付款。因此，Apple 不会向商户披露你的实际信用卡号码，而付款时也不必传送这些资料。

Google Pay

虚拟账户号码是唯一被储存于流动装置上的资料，会经由 Google Pay 传送作为付款交易处理。虚拟账户号码能代表信用卡账户而又有别于真正信用卡账户号码，因此能更保障你的账户资料。

5. 除了我之外，有没有任何人可以使用我的 Apple Pay/Google Pay 付款？

每个拥有你流动装置密码或已在流动装置中登记指纹/Face ID/其他生物辨识凭证(如适用)的人都可以透过 Apple Pay/Google Pay 使用你的信用卡进行认可的交易。你必须保障你的流动装置安全及你的流动装置密码保密。不要让任何人在你已登记信用卡的设备中储存他们的指纹/Face ID/其他生物辨识凭证。请经常保持你的流动装置在上锁状态，以避免第三者使用你的流动装置进行 Apple Pay/Google Pay 交易。避免使用容易取得的个人资料(例如电话号码、出生日期)或简单密码(例如123456)作为密码。你不应以相同的密码接驳其他服务，包括连接互联网或其他网址。

6. 如果我的装置遗失或被盗，应如何处理？

你可致电信用卡报失热线(852) 3603 7899 要求暂时停用已储存于流动装置上的虚拟账户，而你的实体信用卡并不会受影响。你亦可参考本提示 Q14 于 Apple 及 Google 网页查询不时更新的装置遗失或被盗常见问题及解决方案。

7. 如收到续期卡，是否需要更新于 Apple Pay/Google Pay 内的信用卡？

需要。如你之前已于 Apple Pay/Google Pay 登记你的信用卡，当你确认已到期更新的信用卡时，须重新加入该信用卡。于重新加入你的续期卡前请先移除原先已加入 Apple Pay/Google Pay 的旧信用卡。

8. 如收到相同信用卡账户号码之补发卡，我需要于 Apple Pay/Google Pay 之流动装置中进行更新吗？

不需要。如果你收到补发信用卡并有同样的信用卡账户号码、到期日及保安编码，你的流动装置将会自动连接到补发卡之信用卡账户号码。当你收到新的信用卡及确认信用卡后，便可继续使用 Apple Pay/Google Pay 进行交易。

9. 如收到不相同信用卡账户号码之补发卡，我需要于 Apple Pay/Google Pay 之流动装置中进行更新吗？

需要。如果你收到补发信用卡而信用卡账户号码或到期日或保安编码是不相同，你的流动装置是不会自动连接到补发卡之信用卡账户号码。当你收到新的信用卡及确认信用卡后，需要于 Apple Pay/Google Pay 流动装置中进行更新，重新将信用卡加至 Apple Pay/Google Pay 才可进行交易。于重新加入你的续期卡前请先移除原先已加入 Apple Pay/Google Pay 的旧信用卡。

10. 如我重设或更新我的流动装置，会发生什么事？

当你进行资料重设或更新，所有储存在 Apple Pay/Google Pay 中的付款资讯将会被移除。你需要在流动装置重设后，重新设定并加入信用卡至 Apple Pay/Google Pay。

11. 如我更换了我的装置，应如何处理？

如你更换你的装置，包括到新型号，那你需要重新加入你的信用卡至 Apple Pay/Google Pay。请牢记在你的装置买卖、转让或丢弃前，把你的信用卡从装置上移除。

12. 如我需要维修、出售、转让或不再使用流动装置，应怎样处理？

请确保你于维修、出售或不再使用前已经将流动装置上所有信用卡资料移除。及后可于流动装置上重新加入信用卡以继续使用 Apple Pay/Google Pay 应用程式。

13. 我该如何确保流动装置及 Apple Pay/Google Pay 的使用安全？

Apple Pay

使用 Face ID 来验证你的 Apple Pay 交易的建议：

- 请不要从装置设定中停用「使用 Face ID 需要注视萤幕」功能。如果在任何情况下你需要停用此功能，请不要于 Apple Pay 上使用 Face ID；
- 如你有双胞胎或样貌相近的兄弟姐妹，你的兄弟姐妹或可以 Face ID 登入你的 Apple Pay，因此本行建议你不要于 Apple Pay 上使用 Face ID；及
- 如你尚在发育阶段或你的脸部特征可能有所变化，你或不能以 Face ID 登入 Apple Pay，因此本行建议你不要于 Apple Pay 上使用 Face ID。

如你对于 Face ID 的保安存有疑虑，你可使用装置密码来验证你的 Apple Pay 交易。请于「设定」>「Face ID 与密码」>「使用 Face ID」上关掉「Apple Pay」选项。

Apple Pay/Google Pay

无论你使用那一个型号的装置，请参考下列贴士以保护你的流动信用卡：

- 设定锁机密码 - 建议切勿以令人容易猜测得到的个人资料作为锁机密码。
- 请确保所有应用程式从可信任的来源下载。
- 切勿浏览或点击可疑网站或网址连结。
- 当不需要使用时，关闭 NFC 功能(如适用)。
- 更新流动装置的作业系统至最新版本。
- 切勿使用 Jailbreak (越狱) 或 Root 机等手法改装你的装置。
- 请设定时间较短的萤幕自动关闭功能，以防别人盗用流动支付功能。
- 请时常小心看管你的流动装置。

14. 如有其他问题，应如何处理？

有关 Apple Pay 请前往“<https://getsupport.apple.com/>”、有关 Google Pay 请前往“support.google.com/googlepay”或致电信银国际信用卡客户服务热线(852) 2280 1288 以查询信用卡安全、投诉、保安事件或更多资讯。

本通知中英文版本有任何歧义，概以英文版为准。

2025年9月