

澳門金融管理局
AUTORIDADE MONETÁRIA DE MACAU

通函編號 3285/MC010-2025-DSB/AMCM 號

致：澳門
全體銀行

收件人參考
V/REF. 4

日期
DATADA DE

寄件人參考
N/REF. 4

日期
DATA 14 AUG 2025

事項
ASSUNTO: 加強銀行卡網上交易的安全措施

為應對不法分子透過誘騙或竊取客戶銀行卡資料與一次性短訊碼 (SMS OTP)，以進行未經客戶授權的銀行卡網上交易的風險，貴行須於 2025 年 12 月 31 日前 落實以下銀行卡網上交易的安全措施，以更好地保障貴行及客戶的權益：

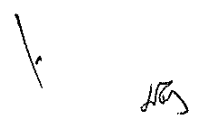
1. 為已開通手機銀行服務的客戶，預設以手機銀行對交易進行驗證。
 - a. 在客戶使用手機銀行進行交易驗證時，透過適當程序以確認為客戶所操作。同時，為提升驗證的便捷性及安全性，儘可能以客戶所持的移動設備（設備綁定）作為確認方式，在客戶進行首次設備綁定或重新綁定時，實施安全嚴謹的設備識別（不可僅記錄設備型號或編號作為後續核對的憑證）和身份驗證（不可僅依賴 SMS OTP 作為綁定設備的單一驗證方式）；
 - b. 確保手機銀行的交易驗證流程順暢和穩定。在實施有關措施前，進行全面的端對端交易測試，並制定機制持續監察驗證流程的每個節點（如監測交易所需完成時間、超時交易的相

關數據、系統承载力等性能指標），以及時偵測倘出現的系統異常或交易失敗情況，以及作適時的跟進及流程的優化；

- c. 提請客戶在首次使用手機銀行進行交易驗證前，預先透過手機銀行開通相應的功能（如手機銀行推送通知功能、設備綁定、生物認證等）；同時，在客戶進行交易時，向客戶提供清晰的交易驗證操作提示。此外，須做好客戶服務支援工作，以及時地回應客戶就交易驗證的查詢和提供倘需的協助。
2. 就暫未開通手機銀行服務或有合理需要的客戶，仍可為客戶提供 SMS OTP 交易驗證方式，惟須實施更嚴謹的交易監控，如在系統增加實時交易監控功能，以提升阻截懷疑欺詐交易的及時性及有效性。同時，應借助執法機構、卡組織或相關行業組織等發佈的詐騙情報，持續優化交易風控模型，以更好地應對不斷演變的詐騙手法；
 3. 在交易驗證過程中，不論採用何種驗證方式，須向客戶清晰展示（尤其在手機銀行頁面，以粗體、不同的顏色及放大字體等設計）有助其辨識有關交易的資訊，包括“銀行卡尾 4 位號碼”、“交易貨幣”、“交易金額”及“商戶名稱”。同時，儘可能在驗證頁面及 SMS OTP 短訊內容上加入“交易序號”，以便客戶核對及確認當前交易；
 4. 完成交易後，須向客戶發出即時短訊交易通知，並儘可能透過電郵發出交易通知（適用於已登記電郵地址的客戶），以及持續鼓勵尚未提供電郵地址的客戶進行登記。

倘若 貴行因特殊情況而未能如期落實上述安全措施，須儘快與本局做好溝通，並須設有相應的風險緩釋措施。

另特此提醒， 貴行須持續透過不同渠道（尤其在官網、網上／手機銀行內的當眼位置），做好銀行卡安全使用及防詐騙資訊的宣導及客戶教育工作，並積極推動客戶下載手機銀行及善用 APP 內查閱銀行卡最近交



易記錄、銀行卡安全及限額管理等功能（請見本局 2023 年 12 月 28 日第 5037/MC017-2023-DSB/AMCM 號通函所要求的“進一步加強銀行卡安全及客戶保障措施”，包括向客戶提供便捷渠道自行關閉或重啟網上交易功能、下調信用額度、即時凍結或掛失銀行卡等功能），以便客戶更安全地使用銀行卡服務。

如有疑問，請派員聯絡本局銀行監察廳李嘉麗女士或曾家豪先生（電話：8395 2369 / 8395 2312，電郵：dsb@amcm.gov.mo）。

此。順頌
商祺

澳門金融管理局
行政管理委員會委員



劉杏娟

銀行監察廳副總監



何仲華