

說明：本期重點內容摘譯自 Nilson Report - 2026 年 1 月第 1299 期之「2030 年全球國際支付卡品牌交易筆數預測」及「生成式 AI 引發的新型詐騙」等 2 篇。

本期重點摘譯：

一、 2030 年全球國際支付卡品牌交易筆數預測

預測到 2030 年，由銀聯 (UnionPay)、Visa、Mastercard、美國運通 (American Express)、JCB、Discover 以及大來卡 (Diners Club) 等全球國際主要支付卡品牌所發行的支付卡，其消費交易筆數將達 1.146 兆筆，較 2025 年成長 35.7%，預計增加 3,014.8 億筆交易，統計範圍包括一般信用卡、商務信用卡、轉帳卡及預付卡等卡種，並包含面對面交易 (Card-Present) 與非面對面交易 (Card-Not-Present) 兩類型態。

從區域別觀察，亞太地區為全球最大消費交易市場，預計至 2030 年消費交易量將達 5,185.6 億筆，較 2025 年成長 35.4%，該地區發行的支付卡預計將占全球消費交易總量的 45.25%，並較 2025 年增加 1,356.1 億筆。

本文所呈現的 2030 年 1.146 兆筆交易，未納入各國的國內自有品牌卡，如 Mir(俄羅斯)、Elo(巴西)、Verve(奈及利亞)及 RuPay(印度)等。

二、 生成式 AI 引發的新型詐騙

要打擊利用 AI 進行詐騙的犯罪分子，唯一的方法，就是以更具策略性的 AI 防禦來對抗 AI 攻擊。支付卡產業的防詐團隊，近年已成功運用 AI 扭轉詐騙曲線，以詐騙損失占交易總額 (消費與現金交易合計) 的比例衡量，2024 年詐騙損失降至每 100 美元 0.064 美元，低於 2023 年的 0.066 美元。

然而，一項新的變數正在發生，持卡人運用生成式 AI，透過來自 Visa、Mastercard、PayPal 及其他公司的協定，建立自主購買代理 (autonomous buying agents)。該環境使犯罪分子得以在銀行、電子商務平台 (包含市集與博弈業者) 及獎勵平台 (如航空公司、線上博弈與線上旅遊業者) 中從事詐騙行為。

生成式 AI 技術，讓犯罪分子能以規模化方式，繞過既有 AI 防詐系統的數位身分驗證與身分認證能力。生成式 AI 的強大能力，也催生出一種全新戰術——同時發動數千筆假交易，迫使防禦方在短時間內耗盡防詐資源，藉此找出系統弱點，再發動第二波精準攻擊以入侵系統。對防禦方而言，真正的挑戰在於：為了容納合法的代理式商務 (agentic commerce)，系統已無法再拒絕所有試圖進入的機器人。防詐與資安團隊如今必須專注於判斷每一個 AI 代理的「意圖」，究竟是夥伴，還是敵人？防詐人員認

為，目前超過 40% 的詐騙嘗試已與 AI 有關。

Darwinium 由 ThreatMetrix 創辦團隊所成立，正是為了因應支付卡產業在這個新時代所面臨的威脅。Darwinium 每月分析 2.5 億筆交易，累積的實務經驗顯示，惡意 AI 代理的行為模式，與合法消費者使用的 AI 代理存在可辨識的差異。該公司協助客戶透過辨識這些細微差異，找出意圖詐騙的機器人。

該公司宣稱其技術可提升 30% 的機器人偵測率、幾乎完全消除簡訊釣魚攻擊 (Short Message Service, SMS)、辨識用於帳戶對帳戶 (Account-to-Account, A2A) 詐騙的人頭帳戶，同時詐騙損失可減半，營運成本降低 40%，且在此情況下仍可正確辨識 99.95% 的回訪客戶。