

說明：本期內容摘譯自 Nilson Report - 2024 年 5 月第 1263 期之「Mastercard 的防詐新服務 Scam Protect」。

本期重點摘譯：

一、Mastercard 的防詐新服務 Scam Protect

專業罪犯使用 AI 軟體及竊取之民眾個人資料，對全球消費者進行詐騙，這使得金融機構採取史無前例的行動來保護他們的客戶。相關的詐騙行為，甚至可以中斷有效客戶的資金匯款。

帳戶對帳戶(account-to-account，簡稱 A2A)的交易是一種相對較不受保護的支付管道，但帳戶交易的日益普及與資金即時結算的特性，卻吸引了老謀深算的犯罪份子。為了打擊 A2A 詐騙與卡片詐欺，Mastercard 推出了新服務「Scam Protect」，這是一套由 AI 驅動身分識別、生物辨識、開放銀行並具其他 AI 功能的新服務，可用來保護消費者，以及那些為消費者發行卡片、開立帳戶的金融機構。

針對 A2A 交易，Scam Protect 服務中，其中一個功能「Mastercard Consumer Fraud Risk」，是允許銀行介入即時匯款，並可在資金匯款前，阻止匯款匯到詐騙集團手上。目前英國已有十家銀行正在使用此功能。Mastercard 正和 Verizon 及全球反詐騙組織(Global Anti-Scam Alliance)等機構進行合作，並將會和 Verizon 共同研發新工具以防堵詐騙。

由於民眾遭到詐騙集團煽動，「主動」進行匯款，因此防止非本人匯款的相關保護機制，如：雙因子認證(two-factor authentication)、一次性密碼(one-time password)等身分認證流程，通常無法起到保護作用。有時，受騙民眾會相當堅決地要進行匯款，以致於不接受防詐提醒訊息，甚至覺得這些詐騙份子應該要得到他們所匯出去的錢。這種客戶本人「主動」匯款給詐騙集團而金融機構卻試圖阻攔所造成的摩擦，讓金融機構感到進退兩難。

Scam Protect 的機器學習及 AI，可透過人們設備上的智慧化及行為上的生物辨識，來判別民眾正受騙上當的跡象，這些受騙跡象包含了民眾在網站或手機 APP 輸入資料時，出現停頓，而這樣的停頓，有時是因為受害者正在接受詐騙集團的遠端電話操控。

Scam Protect 的客製化套裝解決方案，可以傳送風險分數與風險警訊予金融機構，而金融機構同樣需要可即時提醒客戶的工具，向客戶動之以情，放慢疑似詐騙的 A2A 交易

匯款流程。有些交易甚至需要金融機構打電話告知受害者可能正在進行詐騙集團所要求的匯款。

未來的服務發展，將會允許 Mastercard 提供相關洞察資訊給收款銀行，以監控匯入款項並偵測潛在的詐騙行為。Scam Protect 的服務可透由 Mastercard、或透過金融機構詐欺平台整合、以及第三方詐欺防制供應商來取得。