

科技運用於消費者保護：數位時代金融消費者的權益與風險

中原大學財經法律學系蔡鐘慶副教授

一、數位金融浪潮下的金融消費者保護新思維

隨著人工智慧 (Artificial Intelligence, AI)、分散式帳本、開放銀行及大數據運算的迅速發展，全球金融體系經歷了典範轉移。傳統以實體分行、臨櫃面對面為核心的金融服務型態，已轉型為跨越時空限制、強調「隨時隨地的數位化金融生態」。演算法驅動的自動化決策與生成式 AI (Generative AI)，更使金融服務從「客戶主動搜尋」轉變為「系統主動預測並創造需求」。這場數位革命在大幅降低交易成本、擴展普惠金融的同時，亦重構了金融機構與消費者之間的權力關係與資訊結構。演算法黑箱、資料監控、深偽詐欺與介面操縱等新興風險隨之萌生，導致傳統金融消費者保護機制面臨前所未有的制度性挑戰。

科技具有鮮明的「雙刃性」：它既是強化消費者保護、提升監理效能的關鍵賦能工具也是侵害消費者權益的新型風險媒介。本文試圖剖析數位金融環境下的新興風險樣態，探討如何運用法遵科技與監理科技強化消費者防護，並結合實務現況，釐清消費者的法定權益、救濟途徑與自保防線，以期為建構「以人為本、兼顧創新與公平」之金融生態體系提供理論與實務指引。

二、數位時代金融消費者的新興風險光譜

在數位化與演算法高度介入的金融交易環境中，消費者面臨的風險不再侷限於傳統的「資訊不對稱 (Information Asymmetry)」，更進一步擴展為「技術不對稱 (Technological Asymmetry)」，主要風險態樣可區分為下列四大面向：

(一)、演算法黑箱與自動化決策風險

金融機構廣泛運用機器學習模型進行信用評分 (Credit Scoring)、自動化核保、動態定價與智慧投資顧問 (Robo-advisor)。然而，深度學習模型的多層神經網路往往形成「演算法黑箱」，連系統開發者亦難以完全還原其決策推導邏輯，此一特性衍生出兩大法律風險：

1. 演算法偏見與歧視：常見的演算法偏見，包括原先的訓練資料就存在歷史歧視、採樣不足、標註者偏見等問題，由此訓練的模型，自然而然就會「不公平」，還有一種歧視的產生，是標籤偏差，例如有銀行或保險公司，拿過去成功取得貸款或核保的結果當標籤，其結果就是持續複製不公平¹。

¹ 林安妮，小心金融歧視 / 演算法偏見 須矯正，經濟日報，2025年9月17日，available at <https://udn.com/news/story/7239/9009666> (最後瀏覽日：2026.8.15)

2.說明義務履行的困難：依據《金融消費者保護法》第 10 條，金融機構對消費者負有說明商品、服務重要內容及風險之義務。在演算法黑箱下，業者難以向消費者合理解釋自動化決策之具體理由（如貸款遭拒或保費費率加成），很容易侵害消費者的知情權與抗辯權。

（二）、個人資料過度蒐集與數位足跡濫用

金融科技與開放銀行的推進，使得金融機構與第三方服務提供者（Third-Party Providers, TPPs）間的資料共享日益頻繁。部分金融科技應用程式藉由分析消費者的社群互動、GPS移動軌跡、瀏覽紀錄等非金融替代性數據建立信用圖像，此舉往往超越金融服務目的之合理必要範圍，違反《個人資料保護法》第 5 條規定之比例原則：「個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。」此外，跨機構資料串接之資安漏洞，當資料透過應用程式介面（API）頻繁傳輸，若串接之第三方業者資安防護薄弱，易形成資安斷點，導致大規模個資外洩，進而成為下游詐欺集團精準釣魚的資料庫，以2026年5月，SHADOW-AETHER-015外洩了50個國家共8,809家Canvas客戶的資料，這起事件的起因似乎是Canvas的母公司Instructure的平台後端系統遭駭客入侵所導致。此次外洩事件影響了全球各地的大專院校、幼稚園至高中（K-12）學區，以及教學醫院，其中包括八家常春藤聯盟（Ivy League）學校。由於Canvas會儲存個人揭露的敏感資訊，例如：住宿申請時的醫療資料以及與顧問的私人對話，因此其最大風險在於假借真實機構名義的高度針對性魚叉式網路釣魚²。至於立即性的風險則包括：後續的社交工程攻擊、登入憑證濫用，以及針對性網路釣魚攻擊，類似的情形也發生在國內，如國內著名的某集團旗下電子錢包驚傳遭駭客入侵，350萬名用戶個資外洩，引發立委關注，尤其量子電腦正崛起，民間駭客無所不在，引發「AI海嘯」疑慮。金融監督管理委員會（下稱金管會）要如何強化AI資安人才建置，金管會主委彭金隆指出，因應量子電腦，金管會已經發布「金融業後量子密碼遷移參考指引」，未來也會持續跟金融機構協力³整備相關作業。

（三）、新型態科技金融詐欺與社交工程攻擊

生成式AI技術的普及大幅降低了犯罪門檻，金融詐欺已從傳統群發簡訊進化為高度客製化、深偽擬真的複合型攻擊，詐騙集團利用生成式影音技術偽造親友、企業高層或理財專家之容貌與聲紋，或破解金融機構遠端開戶之辨識防線，盜取帳戶權限。甚至利用虛擬資產（Virtual Assets）之匿名性、去中心化與跨國流動特性，包裝「高收益、零風險」的假投資平台，事後資金追蹤與司法管轄難度極高。根據國際刑警組織與資安機構最新數據，AI雖尚未全面「自動化」犯罪，但已顯著提升詐騙效率，使金融犯罪利潤暴增。目前技術門檻的降低主要體現在讓非專業人士也能利用生成式AI消除語言隔閡或製作深偽影音，技術轉折點預計將出現在「代理式AI」（Agentic AI）成熟之際，屆時AI將具備自主拆解任務、協調外部資源甚至指派人類執行實體任

² Trend Micro，從 Canvas 大規模外洩事件，看教育產業的供應鏈資安風險，available at https://www.trendmicro.com/zh_tw/research/26/e/What-Is-the-Instructure-Canvas-Breach.html（最後瀏覽日：2026.8.15）

³ 孫彬訓、魏喬怡，Pi錢包350萬用戶個資外洩 金管會攜手金融業強固資安，工商時報，2026年7月1日，available at <https://www.ctee.com.tw/news/20260701701003-430301>（最後瀏覽日：2026.8.15）

務的能力，當AI從單純的內容生成工具演變為具備組織能力的「犯罪策劃者」，傳統以人為核心的防禦體系有可能將面臨崩潰⁴。

（四）、介面誘導與暗黑模式

數位產品介面設計利用行為經濟學漏洞，透過「暗黑模式」誘導消費者做出非理性金融決策，數位微型信貸透過簡化審核、一鍵支付等機制消除消費摩擦力，使風險感知能力較弱之年輕族群陷入過度消費與多頭借貸陷阱。2022年，美國FTC彙整研究成果及實務案例，發布了名為《揭露暗黑模式 (Bringing Dark Patterns to Light)》的文件。依該文件所示，「暗黑模式」一詞乃是由使用者設計專家 Harry Brignull 於 2010 年創造，用於描述「欺騙或操縱用戶做出他們原本不會做出的選擇並可能造成傷害的設計實踐」……涉及違法風險的常見暗黑模式設計元素，包括以下四大種類：一、引發錯誤認知；二、隱匿或延遲揭露重大資訊；三、導致在未經授權的情況下收費；四、掩蓋或破壞隱私選擇⁵。

三、金管會發布「金融業運用人工智慧 (AI) 指引」

金管會於2024年6月30日發布「金融業運用AI指引」主要分為總則及6大章節，其中總則主要說明AI相關定義、AI系統生命週期、風險評估考量因素、以風險為基礎落實核心原則的方式、第三方業者的監督管理等共通事項；6大章節則分別說明金融業在落實6項核心原則時，依AI生命週期及所評估的風險，宜關注的重點以及可採行的措施，包括目的、主要概念，以及各原則相應的注意事項、落實方式或採行措施等。以下針對金融機構所關注的事項，說明指引的重要內容：

（一）前言：

為利金融機構彈性選擇適宜的風險管理措施，明訂「金融機構可依AI系統具體使用情境所涉風險，依各核心原則宜注意之事項，合理選擇緩解風險之機制及落實方法，包括採取更具成本效益之方法達成目的」⁶。

（二）總則章：

針對第三方業者的監督管理，金融機構重視責任的分工，因此明訂「金融機構運用AI系統時宜辨識可自行監控風險的程度，並對自身較無控制權的部分或事項，透過契約等方式與合作廠商明訂風險監控的責任分工」，並明訂金融機構委託第三方業者導入AI系統相關作業時宜採行的監督管理措施，包括就停止委託的情形，訂定適當的資料或系統遷移機制等。金融機構運用AI系統時，係以風險為基礎落實核心原則，為利金融機構評估風險宜考量的因素，指引中列舉例子供

⁴ 科技新報，AI 尚未降低犯罪門檻，技術轉折點何時出現？，available at <https://cdn.technews.tw/ai-agent/hackers-hate-ai-slop-even-more-than-you-do/7407/>（最後瀏覽日：2026.8.15）

⁵ 歐陽弘，數位化交易介面的設計，應留意「暗黑模式」涉及的競爭法風險，2025年10月3日，available at <https://www.btlaw.com.tw/h/newsinfo?key=0227079976&cont=503416>（最後瀏覽日：2026.8.15）

⁶ 金融監督管理委員會，金融業運用人工智慧 (AI) 指引，2024年6月30日，頁1。

其參考，並明確說明「所舉例子係為協助說明風險評估情境，非就相關使用情境之風險等級加以規範，運用AI系統之風險高低仍由金融機構綜合考量各風險評估因素後自行判斷」⁷。

（三）本指引六大章節簡述如下：

第一章：金融機構的風險管理可能涉及外部審查，為提供金融機構彈性依本身專業及資源程度，採行審查機制，明訂「金融機構可於評估AI系統風險、內部資源及專業程度後，視需要得建立由具AI專業之獨立第三人進行審查、評測之機制」。第二章：考量金融機構不盡然能掌握生成式AI產出之結果，但為確保AI系統的公平性及人類可控，明訂「**金融機構使用第三方業者開發之生成式AI，如無法掌握訓練過程及確保其數據或運算所得出之結果符合公平性時，金融機構對其產出之資訊，仍需由其人員就其風險進行客觀且專業的管控**」。第三章：為保護客戶隱私，參考歐盟「一般資料保護規則」（GDPR），說明金融機構應採用「資料最小化原則」，避免蒐集過多或不必要的資訊，其中「**資料最小化**」係指「**蒐集個人資料必須適當、相關且於資料處理目的之必要範圍內**」。第四章確保系統穩健性與安全性，金融機構在運用AI系統時，必須確保其系統之穩健性與安全性，以避免對消費者或金融體系造成損害；若金融機構運用第三方業者開發或營運之AI系統提供金融服務，應對第三方業者進行適當之風險管理及監督。第五章落實透明性與可解釋性，金融機構在運用AI系統時，應確保其運作之透明性及可解釋性；金融機構使用AI與消費者直接互動時，應適當揭露。第六章促進永續發展：金融機構在運用AI系統時，應確保其發展策略及執行與永續發展之原則相結合，包括減少經濟、社會等不平等現象，保護自然環境，從而促進包容性成長、永續發展及社會福祉。金融機構在AI系統運用過程中，宜對一般員工提供適當之教育及培訓，促進員工能適應AI帶來之變革，並盡可能維護其工作權益⁸。簡而言之，技術可以外包，但風險與保護消費者的責任絕對不能外包。**金融機構必須透過「獨立審查、人類最終管控、資料最小化、資訊揭露」等手段，將AI帶來的技術未知風險（如黑盒子、幻覺、偏見）降到最低，以達到永續經營與保護消費者的雙重目標。**

四、金管會發布「金融資安韌性發展藍圖」

金管會於2025年12月30日發布「金融資安韌性發展藍圖」，強化金融資安生態系與營運韌性，讓數位時代金融消費者的權益獲得更多的保障並降低相關風險，「金融資安韌性發展藍圖」以目標治理、全域防護、生態聯防、堅實韌性為四軸架構，訂有29項措施，目標是建構「可預測、可防禦、可復原」的金融生態系。謹說明十大重點如下：一、強化經營階層資安治理職能與問責機制，鼓勵資安法規調適。二、加強資安人才培育與交流，從共通基準邁向策略目標。三、資安左移，安全納入設計。四、推動零信任架構，提升資安防護基準。五、強化資安監控及防護有效性。六、前瞻部署，因應新興科技的挑戰。七、強化供應鏈資安，健全金融

⁷ 同前註，頁3。

⁸ 同前註，頁6-25。

資安生態系。八、加強資安情資分析與協同防禦。九、辦理資安攻防演訓，強化資安事件應處能量。十、強化多層次備援機制，確保關鍵金融服務可用性⁹。

其中第五點強化資安監控及防護有效性：金管會自2020年起即鼓勵金融機構建置資安監控機制（SOC），並研析駭客組織攻擊手法，制定金融資安監控及組態基準，提供金融機構參考運用，將持續擴增資安監控及組態基準涵蓋範圍（包含雲端），及鼓勵金融機構定期檢驗資安監控及防禦部署之有效性。特別重要的是第六點的前瞻部署，因應新興科技的挑戰：考量AI系統的資安風險更複雜與隱蔽，將研訂金融業AI系統安全防護及檢測參考指引，以涵蓋傳統網路威脅及AI特有攻擊類型；另因應量子電腦已證實對「非對稱式加密技術」構成嚴重威脅，影響網路交易、電子簽章及身分驗證等加密安全，將研訂金融業後量子密碼學（PQC）遷移參考指引，提供金融業據以建立PQC遷移計畫，及視量子電腦及PQC發展成熟度適時推動金融機構辦理PQC遷移作業，更加能確保科技運用於金融消費者之保護。

此外上述「金融資安韌性發展藍圖」第七點強化供應鏈資安，健全金融資安生態系：因應金融業對於第三方服務供應商與外包商的依賴程度日益加深，規劃依產業特性、供應商接觸資通系統之類別及資料敏感度等面向進行分級，研訂資安責任之委外契約參考條款，並鼓勵金融機構建立供應鏈風險評估機制，與其關鍵供應商、第三方服務商、系統整合商等上下游合作，分享威脅、保護資訊、強化控管，聯合資安演練，降低整體供應鏈的資安風險，更加能保障數位時代金融消費者的權益。

五、代結論

為強化與金融科技新創團隊交流互動，傾聽業者對金融科技發展之建議，金管會彭金隆主委於2026年5月20日、6月4日及6月17日，在金融科技創新園區舉辦三場「主委與新創有約」座談會，與29家不同領域的金融科技新創團隊面對面交流，與會團隊分享創新發展過程中所面臨的困境與需求，並由彭主委親自回應，期能共同攜手推動金融科技創新發展。彭主委指出，面對人工智慧、虛擬資產及新科技應用快速發展，金融市場將逐步朝向傳統金融、數位金融及區塊鏈金融三軌金融並行發展。金管會將持續推動FinTech Space 2.0，透過階梯式培育機制及跨域資源整合，為不同發展階段的新創團隊提供精準支持，打造互助共享的金融科技生態系。同時，面對新科技應用趨勢，金管會將秉持「不躁進、也絕不落後」原則，在兼顧風險管理與金融韌性的前提下，以「安全」與「發展」並進的策略，讓創新發展在可承受風險的基礎上穩健前行¹⁰。

⁹ 金管會發布「金融資安韌性發展藍圖」，強化金融資安生態系與營運韌性，2025年12月30日，available at https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202512300002&dtable=News（最後瀏覽日：2026.8.15）

¹⁰ 金管會「主委與新創有約」三場面對面座談，傾聽建言並期勉共同推動金融科技發展新聞稿，2026年7月8日，available at https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202607080001&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,ou=fsc,c=tw&dtable=News（最後瀏覽日：2026.8.15）

此外，中華民國期貨業商業同業公會詹正恩理事長於2026年會員大會上指出公會將秉持「精進制度、有效溝通、共榮發展」理念，扮演主管機關與業者間的溝通橋梁，推動商品創新及制度優化。過去一年提出微小型商品、周五到期臺指選擇權及夜盤交易商品擴增、主動式期貨ETF及槓桿交易商品等多項建議，持續提升市場效率及國際競爭力。金管會副主任委員陳彥良表示，近年全球金融市場受到地緣政治、人工智慧（AI）發展、通膨及主要國家貨幣政策等因素影響，市場波動加劇，也提升投資人對期貨商品避險及資產配置的需求，金管會將秉持「安全與發展並進」的監理理念，持續精進交易及風險管理制度，推動亞洲資產管理中心政策，並透過金融行動創新法規調適平台廣納市場建言，協助商品創新與法規調適，同時持續推動打擊金融詐騙、強化異常交易監理及金融消費者保護。臺灣期貨交易所董事長吳自心亦表示，今年AI產業快速發展及國際市場波動帶動期貨交易量大幅成長，也讓風險管理的重要性更加凸顯。針對調整後淨資本額比率（ANC）議題，期交所已完成緊急因應措施，未來將持續與主管機關及期貨公會研議制度優化，並評估導入國際風險管理制度¹¹。

綜上所述，數位時代的金融發展，必須落實金管會「安全與發展並進」的監理理念。金融創新雖然賦予消費者更多元的投資管道與權益，但消費者亦須體認到，在享受數位便利的同時，伴隨而來的市場風險與詐騙風險也更具隱蔽性，透過公會扮演好有效溝通橋梁、主管機關與金融消費評議中心落實金融消費者保護、交易所完備風險應變措施，以及消費者自身提升數位金融素養，方能在打造臺灣成為「亞洲資產管理中心」的道路上，真正實現創新紅利與風險防範的共榮發展。 

¹¹ 王姿雅，期貨公會會員大會 圓滿落幕，工商時報，2026年7月2日，available at <https://www.chinatimes.com/newspapers/20260702000539-260209?chdtv>（最後瀏覽日：2026.8.15）