欧盟以信息共享为中心的支付反欺诈监管改革镜鉴

王瀚婷　尚博文

摘　要　随着数字科技深度赋能金融服务市场，支付反欺诈问题成为新时代中国金融高质量发展的重要挑战。欧盟建立了以《支付服务指令》为核心的监管框架，但强客户身份验证机制无法应对新型“身份冒充欺诈”问题，信息泄露与监管一致性问题成为支付反欺诈监管的阻碍。对此，欧盟新一轮改革在事前注重信息监控机制建设与客户教育，事中推动服务商及时共享欺诈信息，事后完善受欺诈客户索赔，从而在支付反欺诈与客户信息保护间取得了平衡，但也存在数据处理合法性基础的弊病。我国应当将“信息共享”作为支付反欺诈的中心，注重信息共享法律体系建设与境内外各机构监管合作，进一步推动支付反欺诈监管的“技防”转向。

关键词　金融欺诈　支付欺诈　欺诈监管　信息共享　信息保护

一、引言

党的二十大报告提出，要加强和完善现代金融监管，强化金融稳定保障体系，依法将各类金融活动全部纳入监管。科技是发展的利器，也可能成为风险的源头。数字经济时代，支付体系中融入大量以大数据、人工智能、区块链为代表的科技元素，在推动支付服务更加便捷、高效与精准的同时，也暴露出个人信息、企业信息滥用和泄露问题，形成了跨境经营的电信网络诈骗灰黑产业链条，支付反欺诈问题成为新时代中国金融高质量发展的重要挑战之一。2022 年 9 月出台的《中华人民共和国反电信网络诈骗法》，是对支付欺诈这一特定领域犯罪进行深入治理的专门性、综合性法律，围绕金融欺诈乱象规定了“金融治理”专章。不过，这部法律中有关支付反欺诈监管逻辑、监管合作与技术应用等问题还有待学理反思。面对日益现代化、科技化、数据化的支付市场，欧盟针对相关的困境与挑战，于 2023 年开启了新一轮支付反欺诈改革。本文通过分析欧盟支付反欺诈监管的历程、困难、改革及其亮点和局限，为中国支付反欺诈监管提供制度优化的建议。

二、欧盟数字化时代支付反欺诈监管演变及现实困境

（一）欧盟支付反欺诈的监管历程与基本框架

在支付领域，欧盟建立了以《支付服务指令》（Payment Services Directive，PSD）为核心的监管框架，并根据市场发展与监管效果不断更新迭代。欧盟议会于

王瀚婷，对外经济贸易大学法学院；尚博文（通信作者），对外经济贸易大学法学院、涉外法治研究院助理教授。

2007 年审议通过第一版《支付服务指令》（PSD1），将刺激欧洲的竞争、提高服务质量和保护消费者作为其立法目的，旨在规范所有欧洲经济区成员国的支付服务及其提供商（European Commission，2018）。PSD1 创造性地引入了支付服务提供商（PSP）这一概念，放宽了新市场进入者和支付机构的准入条件。相较于其防范打击欺诈、保护消费者的功能，PSD1 更注重通过管理和激励欧盟各成员国的支付系统，简化服务流程并提高欧盟地区的支付服务效率，协调整个欧盟单一市场的支付交易。

随着欧盟电子支付市场的不断发展，大量新型支付中介机构与支付形式挑战了以 PSD1 为主体的监管框架，欧盟的电子支付市场中出现了更为复杂、形态各异和风险传导性更强的支付欺诈行为。2019 年，欧盟银行卡欺诈损失金额高达 18 亿欧元（European Central Bank，2021）。对此，修订后的第二版《支付服务指令》（PSD2）于 2018 年 1 月生效。PSD2 将新型支付中介与支付形式全部纳入监管，规定了两个新的“第三方服务提供商”，一是账户信息服务提供商，提供收集和整合用户在不同银行账户信息的服务；二是支付发起服务提供商，在用户授权后获取支付账户的访问权，并帮助用户发起资金支付或资金转移。

PSD2 有效地提高了支付反欺诈监管力度，被认为“更好地保护支付服务用户免受欺诈、滥用和支付问题的侵害”，其中的代表性举措就是“强客户身份验证”（Strong Customer Authentication，SCA）。PSD2 第 97 条要求银行在“客户在线访问其支付账户、发起付款或通过远程渠道采取任何可能意味着支付欺诈或其他滥用风险的行动”时，都要应用强客户身份验证机制，通过技术安全机制在欺诈发生之前介入干预。强客户身份验证机制将身份识别形式分为用户知道的信息（如密码、个人身份识别码等）、个人设备（移动终端、银行卡等）以及个人特征（人脸、指纹）这三项独立要素，某一个要素的违反不会损害其他要素的可靠性。强客户身份验证机制要求支付机构通过至少两项因素身份验证，满足“双重认证”后才能执行电子支付，确保“每当客户访问他的账户或发起交易时，支付处理机构都会确认他同意交易”（Fracassi & Magnuson，2021）。

此外，面对大量涌现的金融科技公司等市场参与者，PSD2 不仅在支付反欺诈的硬性监管规则层面有所突破，还引入了具备创新性和颠覆力的“开放银行”（Open Banking）制度。数字经济的发展也为开放银行与第三方的支付服务合作提供了基础，从而使其带有互联网金融产品的特质（杨东和程向文，2019）。“开放银行”要求银行等第三方服务提供商（Third Party Provider，TPP）在获得客户明示同意后，得以访问该客户的银行账户及账户信息，使 TPP 能够为用户提供个性化、多样性的账户信息和支付启动服务。通过减少银行客户的锁定效应（Lock-in Effect）[①]、支持支

① 锁定效应是指因转移成本巨大或转移造成不便利，消费者往往在特定服务上依赖于单一供应商而不会转而选择其他供应商。

付领域的科技与业务创新，PSD2 意在以促进性制度探索更为高效、全面的支付反欺诈监管模式。

（二）数字化时代欧盟支付反欺诈的监管挑战

PSD2 在支付反欺诈与支付科技创新领域的监管成效显著。不过，PSD2 实施五年以来，随着大数据、区块链、人工智能等技术深度赋能支付服务，欧盟支付反欺诈监管迎来了全新变化。移动支付打破了传统支付的限制，已成为互联网时代最为便捷的支付方式（屈淑娟，2021）。从欧盟委员在 2023 年 2 月发布的 PSD2 应用和影响研究报告来看，客户面临欺诈风险、对支付缺乏信心仍然是欧盟支付市场存在的首要问题。新的数字支付解决方案、支付服务产品的激增以及新的市场进入者等内容，日益暴露出 PSD2 立法和监管框架的局限性。

首先，支付欺诈仍然是欧盟支付市场的关键问题。数字化金融欺诈渗透业务环节较多，手段多样，场景适应性强的特征越发凸显（郝光昊，2019）。欧盟委员会的评估承认了 PSD2 引入强客户身份验证机制对预防支付欺诈的重大积极影响，但强客户身份验证机制无法应对以“Spoofing”为代表的多种新型支付欺诈形式。“Spoofing”意为“身份冒充欺诈”（Impersonation Fraud），指欺诈者冒充客户支付服务提供商的员工，滥用支付服务提供商的姓名、邮件地址或电话号码来获取客户的信任并诱骗付款，这一欺诈方式模糊了不同交易之间是否有经授权之别，目前为止强客户身份验证机制仍然难以防止此类欺诈。鉴于 PSD2 实施以来此类社会工程（Social Engineering）案件数量的显著增加，欧盟委员会认为需要在预防和纠正欺诈方面采取新的反欺诈措施（European Commission，2023）。与之相对应的，客户在经历欺诈后缺乏相应的权利保护与索赔机制，将会进一步降低消费者对支付市场的信心与信任程度。

其次，虽然 PSD2 开启了“开放银行”这一共享客户信息与鼓励支付创新的先河，但可能加剧泄露客户信息并被欺诈者利用。以开放银行中的屏幕抓取技术（Screen Scraping）为例，用户首先需要向第三方服务提供商提供完整的银行账户名、密码等登录凭证信息，后者利用这些信息能够代替用户登录银行账户，通过手动或自动化方式直接获取用户银行账户与交易信息，或是直接发起新的支付请求（刘倩，2019）。在此过程中存在以下多个安全漏洞和隐患：欺诈者可能假扮服务提供商获取客户的账户密码；以小微企业为代表的服务提供商会存储客户银行账户用户名和密码，实践中出现了大量第三方应用程序遭受网络攻击、信息被窃取、信息泄露等情形；由于屏幕抓取技术替代登录的特性，监管机构将无法要求银行通过强客户身份验证机制中的“个人特征”要素（如人脸、指纹识别等）来增强身份验证（Nizan，2020），极大降低了支付欺诈的防范能力。

最后，PSD2 的实施暴露出欧盟内部的监管一致性与合作问题。《欧洲联盟运作条约》并未将“指令”（Directive）作为可立即执行的法律，而是需要欧盟各成员国结合自身经济水平、本国机构综合能力等客观情况将有关要求内化于本国法律中。由此，欧盟成员国对 PSD2 的具体实施以及国家主管当局（NCAs）的行政实践在一定程度上引发了国家选择权和自由

裁量权，从而导致对受监管支付服务范围等内容的差异化解释（Michael，2023），部分支付模式、产品和服务出现了行业不确定性，进一步降低了在欧盟境内运营的公司的监管透明度。此外，各国监管当局在针对违反开放银行 API 标准的罚款案例数量和金额存在差异，易导致支付反欺诈监管在欧盟境内执法统一性与威慑力的削弱。此外，德国消费者组织联合会认为，需要促进主管数据保护机构和欧洲银行管理局（European Banking Authority，EBA) 为代表的金融管理机构之间的合作 (Verbraucherzentrale , 2021)。 以 PSD2 为代表的支付监管法，与以《通用数据保护条例》（General Data Protection Regulation，GDPR）为代表的数据保护法之间存在的不协调性，会造成法律的不确定性。

面对日益现代化、科技化、数据化的支付市场，PSD2 中强客户身份验证机制适用范围的有限性、“开放银行”中客户信息泄露与滥用问题，以及欧盟内部监管一致性与合作困境等挑战，促使欧盟委员会开启支付反欺诈监管的反思与重构。2023 年 6 月 28 日，欧盟委员会发布了名为 PSD3 的修订支付市场指令提案，并宣布将建立支付服务法规 (Payment Services Regulation，PSR)，从强化支付反欺诈、改善消费者权利等多方面进行新一轮的监管改革。

三、欧盟支付反欺诈的全流程改革：以信息共享为中心

相较 PSD2 的缺陷，欧盟新一代支付服务改革是全流程性的，将欺诈信息作为开展支付反欺诈监管的抓手，强调收集与监测欺诈信息，并注重将相关信息在企业与客户之间、企业与企业之间共享，完善了支付欺诈行为发生后的索赔与执行。

（一）事前阶段：欺诈信息监控机制与客户教育

信息不对称的市场中，规避监管以获得最大利益的强烈动机促使被监管者提供信息时减损其真实性、全面性等（杨东，2018）。支付欺诈信息共享的前提是高效且及时地获取信息，而支付交易监控机制是获取信息的重要渠道。长期以来，欧洲的支付服务提供商需要遵循以反洗钱和恐怖主义融资（AML）等为由的交易监控要求。例如，Volksbank、Rabobank 等五家荷兰银行联合制订的一项名为“荷兰交易监控”（Transaction Monitoring Netherlands，TMNL）的计划。该计划采用人工智能和机器学习工具来分析来自所有五个银行平台的交易信息，共同监控和报告疑似与恐怖主义、非法军火交易、毒品和人口贩运等犯罪行为相关的异常交易。TMNL 计划扩大了跨银行在交易监控方面的合作，打破不同银行间的“数据竖井”（Data Silos），监测和汇集来自不同银行的海量高价值支付信息。在市场实践与探索的基础上，为了使支付服务提供商能够预防和检测潜在的欺诈性支付交易，PSR 第 83 条规定了“交易监控机制与欺诈数据共享”，要求支付服务提供商建立交易监控机制。交易监控机制应基于对以往支付交易的分析和在线支付账户的访问，重点分析强客户身份验证机制中的三项要素信息、支付账户信息、交易信息以及会话信息等，并根据数据库中已知的欺诈场景、每笔支付交易金额、会话中是否被恶意软件入侵等情况，综合考虑支付风险。PSR 新规定的交

易监控机制意在丰富监管“触手”，能够有效提升支付反欺诈监管的触及度与穿透性，是一种对数字社会生产方式做出的积极调试，也体现出组织社会生产与控制权力一定程度的回归（张凌寒，2022）。

交易监控机制意在提前识别与监测支付欺诈信息，而信息作为传统金融监管理论中一项重要的监管策略，其首要功能是教育消费者，确保其理解金融公司运作模式与产品情况。与金融机构相比，金融消费者存在普遍的认知偏差，其风险承载能力与隔离能力处于显著劣势（钱玉文，2024）。金融风险教育的缺位将恶化公众盲目参与的现象（王鹏民 等，2023）。欧盟委员会认为，操纵和冒充等技术使支付欺诈变得越来越复杂，支付服务提供商需要定期采取必要举措来提高支付服务用户对支付欺诈风险和趋势的理解和认识，从而在加强支付欺诈预防方面发挥重要作用（European Commission，2023）。这种风险教育型的“必要措施”规则反映在 PSR 第 84 条，主要应用在支付服务提供商内部以及服务提供商与客户之间，其中对于内部员工，支付服务提供商应至少每年组织一次有关支付欺诈风险和趋势的培训计划，提升员工应对支付欺诈的素养与能力；对于服务商客户，当新形式的支付欺诈出现时，支付服务提供商需要考虑到最弱势客户群体的需求，通过适当的方式和媒体向其客户发出警报，明确告知客户如何识别欺诈企图、需要采取的必要预防措施以及如何举报欺诈行为。

（二）事中阶段：服务商及时共享欺诈信息

合作打击金融领域欺诈的做法已有诸多先例。英国 2006 年反欺诈法及数字欺诈委员会认为，信息共享“是反欺诈工作的重要组成部分，监管机构和立法机构必须积极鼓励”（House of Lords，2022），英国政府反欺诈战略也将改善信息共享确定为反欺诈工作的一个关键的跨领域主题（HM Government，2023）。有效提取并应用数据中包含的信息是提升微观运行效率的核心（蔡跃洲和马文君，2021），整合共享信息是破解信息壁垒的有效手段（张勇进和章美林，2018）。基于支付欺诈行为的复杂性与技术性，单一的支付服务提供商无法全面了解支付欺诈的所有要素，需要来自其他支付服务提供商识别或监测的潜在欺诈活动的信息，这就对服务提供商之间共享欺诈信息提出了更高的要求。

支付反欺诈的一项重要举措是通过国际银行账户号码（International Bank Account Number，IBAN）对客户姓名进行验证的服务及信息共享。IBAN 是支付服务提供商赋予客户的唯一标识符。2022 年 10 月，欧盟委员会提议修订单一欧元支付区法规，对欧元即时支付的支付服务增加了向用户提供 IBAN 与姓名验证服务的监管要求，PSR 对此进行了扩展与革新。第一，将该监管要求扩展到以欧盟货币提供任何信用转账的支付服务提供商。第二，支付服务提供商需要免费向客户提供唯一标识符的验证服务，即收款人的支付服务提供商需要验证付款人提供的唯一标识符（IBAN 号码）与收款人姓名是否匹配。第三，当有足够的证据推测存在欺诈性支付交易时，支付服务提供商之间可以交换和共享收款人的唯一标识符的相关信息。如果其他提供商的客户是可被视为欺诈的信用转账的付款人，则提供商需要联系客户进一步监控账户。在此情形中，如支付服

务提供商未经详细调查，其与其他支付服务提供商共享的支付欺诈信息不构成取消银行服务的理由。此外，PSR 还要求支付服务提供商建立基于信息共享安排的专用 IT 平台，完善进行信息共享的平台基础设施。在信息共享平台中，建立合作关系的支付服务提供商不仅可以集体使用上述唯一标识符，还能够共享操纵技术和其他与欺诈相关的信息。

除了向客户、其他支付服务提供商共享欺诈信息之外，欧盟委员会还计划建立支付欺诈信息的报告制度。鉴于有效监管缺位会加剧对违法信息报告过程中对于信息传输、信息安全保护的担忧（邱遥堃，2022），欧洲银行管理局作为银行业的监管部门，需要与欧洲央行（European Central Bank，ECB）合作制定有关欺诈报告的统计数据监管技术标准以增强监管的确定性与可预见性。据此标准，支付服务提供商每年应向其主管部门提供与不同支付方式相关的欺诈统计数据。作为反馈，根据支付欺诈风险的新趋势，欧洲银行管理局应制定指导金融机构与客户的支付欺诈风险应对指南。另外，此类信息共享需要符合 GDPR 第 6 条“合法利益”的法律原则，但在实践中对于“合法利益”的界定和把握还未明晰，存在一定争议。[①]

（三）事后阶段：完善受欺诈客户索赔制度

如前所述，PSD2 的一大问题在于缺乏客户被欺诈后的权利保护与索赔机制，难以应对近年来大量“身份冒充欺诈”案件对交易授权认定的挑战。PSR 第 79 条认为，由于欺诈者可以控制整个同意和身份验证过程，支付服务提供商的客户作为弱势者的“同意”只是一种顺从状态的描述（詹姆斯 · 哈克尼，2016），且难以识别其授予同意的方式。而相较客户而言，欧盟立法者认为支付服务提供商可以通过充分预防、与移动网络运营商等电子通信服务提供商联合开发技术保障措施等更多手段来预防遭受欺诈。不过，支付服务提供商在欺诈案件中信息被盗用、所控制的资金被转移以及遭受声誉损失，其实也可以被视为支付欺诈的受害者。进一步来说，无论客户是否授权每笔欺诈交易，如果均要求支付服务提供商对其进行退款，既在经济上成本高昂，还可能导致道德风险并降低客户的警惕性。

PSR 就此问题从行为能力的角度进行了价值权衡与法理考量，完善了客户被诈骗后的退款与索赔制度。首先，当客户在不知情时授权进行欺诈性支付交易，应充分保护客户。如果第三方冒充支付服务提供商员工，利用该支付服务提供商的姓名、电子邮件或电话号码，对其用户进行非法操纵（manipulated），并且该操纵导致后续欺诈性授权支付交易的，在客户发现后立即向警方报案并通知其支付服务提供商后，支付服务提供商应向客户退还欺诈性授权支付交易的全部金额。

其次，如果支付服务提供商有合理理

① 例如，在荷兰皇家草地网球协会诉荷兰数据保护局案（Koninklijke Nederlandse Lawn Tennisbond v. Autoriteit Persoonsgegevens）中，荷兰数据保护局认为“合法利益”仅指那些由法律所确立并由法律所决定的利益，而该协会则认为其范围更加广泛，任何利益只要不违反法律，都可以构成合法利益。

由怀疑客户存在“故意欺诈或重大过失”，则应当提供拒绝退款的理由，并承担相应的证明责任。在这里，欧盟委员会虽然将“故意欺诈或重大过失”的界定诉诸欧盟各成员国的法律，但还是以具体案例呈现出“重大过失”的认定标准。例如，以开放且易于第三方检测的格式将用于授权支付交易的凭证保留在支付工具旁边，就会被认定为“重大过失”；再如，如果客户成为某个欺诈类型案件的受害者后已经收到退款，后续又遭受同类欺诈、向同一支付服务提供商再提出退款请求，表明客户未尽到经历欺诈后应尽的注意义务，可以认定为“重大过失”。最后，如果付款人无法意识到支付工具的丢失、被盗或盗用，则不应承担任何责任。同时，为激励支付服务用户在支付工具被盗或丢失时立即通知支付服务提供商，欧盟立法者对客户施以“50 欧元”的责任承担限度，而且用户一旦做出通知行为，则无须承担因未经授权使用该工具而产生的任何后续损失。此外，欧盟委员会认为电子通信服务提供商有义务为集体打击欺诈做出贡献。在欺诈行为发生后，PSR 要求电子通信服务提供商应与支付服务提供商密切合作并迅速采取行动，实施技术措施保护通信与邮件的安全性和机密性。

四、欧盟支付反欺诈改革启示及其反思

欧盟本轮支付反欺诈改革搭建了事前交易监控与客户教育、事中信息共享、事后客户索赔这一更为全面的治理框架，并依托信息共享创新了一些重要的机制，其中涉及的基本原则、发展方向以及未竟之事值得进行总结与反思。

（一）强调在支付反欺诈与客户信息保护之间取得平衡

从 PSD1 到 PSD3 以及 PSR 的迭代过程，实质上是欧盟展开的一场监管沙盒实验，旨在应对支付欺诈这一典型的信息负外部性问题。客户支付信息收集与处理是通过分析获取支付反欺诈线索的关键，为此 PSR 提出了以信息共享为核心的解决方案，由此带来了如何兼顾客户信息保护的课题，而这一课题与 GDPR 等数据保护法规的原则规定、在支付场景下清晰的责任界定规则和高效的监管合作机制密切相关，贯穿了欧盟支付反欺诈改革的全过程，在提供支付服务、共享支付信息两个环节力求取得反欺诈成效与信息保护的平衡。

在提供支付服务环节，支付服务提供商处理信息的行为符合 GDPR 第 6 条“履行合同所必需”这一合法性基础，要求遵守目的限制、数据最小化等基本原则。PSR 对相关服务提供商施以信息保护的严格责任，以支付发起服务提供商为例，第 46 条对其规定了 4 条信息处理禁令：一是将敏感支付信息作为红线，要求支付发起服务提供商在任何情况下不得储存；二是所处理的信息须以支付发起服务内容为限，不得要求用户提供超出限度的其他信息；三是在支付发起服务目的之外不得使用、访问和储存任何个人与非个人信息；四是禁止修改金额、收款人及交易的其他任何信息。此外，“经由设计的保护”也被认为应当纳入所有支付信息的处理系统中，意图通过技术或服务的物理设计、代码架构等，展现出将“硬法”刻进系统软件的理念（许可，2022）。

在共享客户支付信息环节，为了确保交易监控机制有效发挥作用，存在着由单

一持有者转向两个或多个服务商长期共同持有信息的情形，处理客户信息的类型与时限被特别强调。服务提供商交易监控机制所处理的信息，应仅限于支付服务客户的环境与行为信息、交易账户信息、交易信息与会话信息。同时，支付服务提供商必须为用于预防欺诈的不同数据类型建立相应的保留期限，严格限制在检测特殊或潜在欺诈行为所需的时间内，并定期删除检测欺诈不再需要的信息。此外，在不同服务商的信息共享安排开展前，PSR 特别施加了数据保护影响的事前评估环节，数据保护影响评估表明，在缺乏保障措施、安全措施和风险降低机制的情况下，该处理将对自然人的权利和自由造成高风险，支付服务提供商未经咨询相关数据保护部门不得开展信息共享。为更精准地评估信息共享机制的净社会效益，并动态调整监管强度以实现最优平衡点，可考虑通过一些监测指标持续追踪并评估效用，例如，可将“因信息共享导致的个人数据泄露事件数”与“通过信息共享实现的欺诈交易拦截率”的比值作为核心观测指标，并辅以用户投诉量、挽回经济损失金额等作为辅助指标。

（二）监管注重规则统一、机构协同及科技赋能

首先，为欧盟成员国之间提供了新的反欺诈法律基础。在欧盟本轮支付反欺诈的改革中，PSD3 与其 PSD1、PSD2 一致将以“指令（Directive）”的形式由成员国转化为国家法律，便于就其中激进与创新部分根据各国情况预留空间；与此同时，内容更为成熟、确定性更强的 PSR 则以“法规（Regulation）”的形式出现，力求在单一欧元支付区内提供确定性与一致性，减少反欺诈监管的碎片化与法律障碍。

其次，强调多个跨领域监管机构之间的监管合作与信息共享。监管信息是“宝库”，然而监管机构无法从处于广泛分散状态的信息中收集充分监督和控制金融市场所需的信息（Riccardo，2011）。面对现代支付市场的多样化风险，强调包括市场主体、行业协会和监管机构在内的多主体、多环节协同，使监管信息在不同主体之间共同使用，成为防范支付欺诈、化解金融风险的应对之道。2021 年 12 月，欧盟委员会通过了《欧盟金融服务监管数据战略》（Strategy on Supervisory Data in EU Financial Services），目的是通过高效收集、利用和分析数据，使监管机构之间更融洽地相互协调配合，保障金融体系稳定。除了前述支付服务提供商与电子通信服务提供商、数据监管部门的监管合作外，PSR 第 81 条将欧洲银行管理局定位在监管协调机构位置，强调应促进支付监管机构之间、支付监管机构与欧洲央行、欧盟网络与信息安全局等在支付运营与风险防控领域展开信息共享等方面的合作。

最后，注重支付反欺诈的科技赋能。与帮助金融公司遵守其合规职责的“监管科技”（Regulatory Technology）不同，“监督科技”（Supervisory Technology）指监管人员通过使用技术来提供创新和高效的监管方案，以形成更有效、灵活和响应迅速的监管系统（European Insurance and Occupational Pensions Authority，2023）。对银行监管者持有的大量信息进行技术分析能够获得巨大收益（Pentti，2021），欧盟特别注重支付反欺诈监管中的监督科技赋能。在立法层面，PSR 特别强调交易监控机制中人工智能技术的应用；在实践层

面，欧洲中央银行先是于 2021 年成立了监督科技中心，搭建了 IT 专家与监管部门的合作平台，并于 2022 年 4 月完成超过 2 亿欧元的监督科技采购，大幅扩展了在人工智能、机器学习等领域的监管能力，进一步推动支付反欺诈监管的数字化转型。

（三）改革未涉及数据处理合法性基础的问题

欧盟委员会将新一代支付服务指令视为“将支付和金融部门带入数字时代”的新希望（European Commission，2023）。不过，在明确欧盟支付反欺诈监管进展的同时，也需要看到新规的局限性。最为突出的问题是，作为指令的 PSD3 以及作为法规的 PSR 都还未解决 GDPR 对数据流通的阻碍问题。欧盟通过 GDPR 建立了以个人信息自决权为中心的数据权利保护体系，形成了以数据主体对个人数据有效控制为目标的保护机制（汪庆华，2021），赋予用户访问、查询、更正、删除、被遗忘、可携带等一系列权利。在 GDPR 第 6 条的合法性基础中，“数据控制者或第三人的合法利益”虽然也被视作六项合法性基础之一，但在发生利益冲突时需要优先保护数据主体的权利（郭雳和尚博文，2023）。

GDPR 的重述（Recital）第 47 条认为“出于防止欺诈的目的而严格必要的个人数据处理也构成相关数据控制者的合法利益”，但“合法利益”的基础适用需要存在合法利益、处理行为对于目的的必要性以及“平衡测试”这三个要件（House of Lords，2022）。虽然“合法利益”有时能够作为预防欺诈目的的个人数据处理提供法律依据，但大多数情况下企业仍然会担心无法满足“平衡测试”，仍倾向于“个人同意”作为合法性基础，这将使打击支付欺诈变得更加困难（郭雳和尚博文，2023）。

英国数字、文化、媒体与体育部开展了名为“数据：新方向”的数据保护框架改革磋商，将“合法利益”作为一项关键主题，并提出了一份数据处理活动“白名单”，这些处理行为将自动被视为属于合法利益，从而取消了与合法处理依据相关的行政要求（UK Department for Digital, Culture, Media and Sport，2022）。在数据保护法改革中将支付反欺诈纳入数据处理的正面清单，有望成为推动反欺诈信息共享的未来进路。此外，可以考虑提供可操作的立法补丁弥合 GDPR 合法性缝隙，即在条款中明确规定为防范支付欺诈而共享经过假名化处理的特定交易信息可被自动视为符合 GDPR 下的合法利益，豁免机构进行个案“平衡测试”的义务，但前提是共享行为必须严格遵守数据最小化原则，以达到平衡激励信息共享与保护数据主体权利的目的。

同时，考虑到屏幕抓取技术天然存在的安全性漏洞，PSR 第 45 条将 API 作为唯一的信息共享渠道，严格强制 API 的建设与推广。虽然 API 以规范性与安全性见长，但访问便捷性与效率价值也需要被重点考虑。欧洲银行管理局就曾总结出 PSD2 实施过程中 API 的诸多滞碍，如银行在身份验证过程中嵌入冗杂的同意确认与其他步骤，再如在注册过程、通信过程与强客户认证机制中的技术障碍。欧盟新一轮支付反欺诈监管的成功与否，很大程度上取决于如何在 API 优先的数据访问格局中妥善制定相关具体标准与执行规则。为探索最优技术路径，监管机构可通过对比实验，以评估强制性 API 标准与自愿性监管沙盒两种模式的优劣。例如，可选取部分金融

中心城市和特定机构集群作为试点，一组推行统一 API 数据共享标准，另一组则鼓励在沙盒内探索多元化共享技术。通过比较两组在技术成本、欺诈识别效率、创新产出和安全稳健性等维度的差异，为制定最终技术路线图提供坚实的实证依据。

五、推动我国支付反欺诈监管体系建设的建议

（一）构建支付反欺诈监管的信息共享法律体系

同为支付欺诈，但每个法域的呈现方式与突出问题则因其独特社会禀赋不尽相同。在我国，支付服务的潜在风险被电信网络诈骗产业链利用与放大，截至 2024 年，五年来公安机关共破获电信网络诈骗犯罪案件 194.5 万起，自 2021 年已紧急拦截涉案金额 1.1 万亿元。[①] 以电信网络诈骗为代表的新型网络犯罪已成为当前的主要犯罪形态，深刻地影响了支付行业发展与监管变革轨迹。2016 年以来，人民银行等监管部门从账户分级、资金结算、开户限制、冻结止付与 POS 机五要素合一等多个维度构建了部门规则。[②]2022 年 9 月，《中华人民共和国反电信网络诈骗法》的出台是“小切口”立法形式，成为对支付欺诈这一特定领域犯罪进行深入治理的专门性、综合性法律，并将“金融治理”单列一章，对银行、支付机构提出了具体要求。

面对大数据、人工智能、云计算等技术在支付产品和服务中的全新挑战，欧盟开展的新一轮支付反欺诈监管改革具备重要的借鉴意义，信息共享需要作为反欺诈监管的重要体系。《中华人民共和国反电信网络诈骗法》对电信部门、清算机构、企业账户和涉诈样本信息的共享或查询机制进行规定，体现出对信息共享理念的高度重视。[③] 上述规定通常将权责赋予相应领域的主管部门，要求其应当负责建设信息共享机制。2022 年 8 月，人民银行主管的中国互联网金融协会与多家银行作为联合发起方，共同建设了“基于区块链的金融机构反欺诈风险信息共享系统”，成为科技赋能下欺诈信息共享机制的创新性尝试。建议充分发挥相关行业组织的功能，由其在主管部门的指导下，推动各金融机构与非银支付机构之间的联合行动，将原来以竖井形式分布的各类欺诈风险信息整合应用，形成区域性、行业性的欺诈信息共享机制和平台，构建数字化时代支付反欺诈的国家、社会和企业的协同治理。充分发挥金融治理、互联网治理等多种手段构建与完善治理生态，打破支付欺诈生态平衡，不断压缩犯罪发展空间（刘为军，2023）。

在个人信息保护方面，《中华人民共和国反电信网络诈骗法》第 5 条强调了知悉保密要求，第 16 条、第 18 条均规定相关信息不得用于反电信网络诈骗以外的其他

① 公安部.中国公安机关打击电信和网络诈骗取得重大成功[EB/OL].(2024-05-31).https://www.mps.gov.cn/n2255079/n6865805/n7355741/n7355786/c9594157/content.html.

② 详见《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261号）、《关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2019〕85号）、《中国人民银行关于加强支付受理终端及相关业务管理的通知》（银发〔2021〕259号）等。

③ 详见《中华人民共和国反电信网络诈骗法》第10条、第16条、第17条和第32条。

用途，但相关规定仍然不够详细。现实中仍然存在因部分私主体凭借其优势地位将自身意志强加于其他处于弱势地位的私主体，而产生的不平等私主体间以个人信息权益为代表的基本权利侵害问题（马康凤，2023）。建议一方面将敏感支付信息作为红线，要求金融机构、非银支付机构在任何情况下不得储存，另一方面注重因服务商信息泄露导致的支付欺诈、信息共享损害个人信息权益等不同电信网络诈骗情形下用户的权利赋予与行权渠道，切实保障支付反欺诈全流程中的个人信息权利。

（二）加强机构改革背景下支付反欺诈的监管合作

现代支付欺诈应用网络技术将分割在不同区域的作案空间连接在一起，通过远程、非接触等方式诈骗公私财物，实现了欺诈的空间升格与区域跨越，借助司法管辖区的制度及执法差异增加了监管防范难度（刘为军，2023）。监管合作与协同，成为数字化时代支付反欺诈的必然要求。从电信网络诈骗的监管来看，监管协同与合作成为《中华人民共和国反电信网络诈骗法》的一大特色，即在监管机构层面，建立起以公安机关牵头负责，金融、电信、网络、市场监管等依照职责在各自领域内履行主体责任的格局；在市场主体层面，由电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者建立内控机制与安全责任制度，共同承担风险防控责任。

在金融监管与公安执法的监管合作方面，《中华人民共和国反电信网络诈骗法》特别规定了即时查询、紧急止付、快速冻结、及时解冻和资金返还等创新型制度。从其效果来看，2022 年全国累计侦破电信诈骗案件高达 46.6 万起，紧急拦截涉案资金超过 3 000 亿元。[①] 相较这些成果而言，信息保护部门在其中的参与并不明显，国际执法合作也仅有第 37 条这一原则性规定，有待进一步加强。欧盟支付反欺诈改革中特别注重与信息保护部门的监管联动，是因为信息泄露正是支付欺诈的起因与源头。而且，信息泄露还具备一次泄露、终身损害的特性，甚至敏感信息的泄露可能造成严重的精神损害（谢鸿飞，2021）。对此，首先，建议加强国家网信办与人民银行、金融监管总局等在支付领域全方位的反欺诈信息互通能力和联防能力，建立金融监管与数据保护的执法合作体制机制，以重大、集中性的电信网络诈骗事件或信息泄露事件为切入点，开展现场检查、数据报送等执法活动，对相关信息泄露来源及其责任部门倒查与问责。其次，建议在《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”）对数据来源者权利保护做出的明确要求[②] 之上，加强个人作为数据来源者的权利保护，围绕支付欺诈为个人建立起举报与投诉专项通道。最后，面对电信网络诈骗犯罪呈现出专业化、产业化、集团化和国际化特征，除了完善国内公安、金

① 中国新闻网.国家反诈中心去年拦截诈骗电话15.5亿次止付资金超三千亿元[N/OL].2022-03-05.https://www.chinanews.com.cn/sh/2022/03-05/9693378.shtml。

② 指推动基于知情同意或存在法定事由的数据流通使用模式，保障数据来源者享有获取或复制转移由其促成产生数据的权益。

融、信息等各领域的监管合作外，还应发挥我国在金砖国家、“一带一路”沿线国家的政治影响力，推动签署双边或多边协议，着力加强与其他亚洲国家、国际监管组织和司法机关的支付反欺诈协作。

（三）推动支付反欺诈监管的“技防”转向

从市场与政府的关系来看，支付等金融服务作为一种市场活动，其发展天然就领先于政府规制的步伐。而随着科技创新赋能金融服务，金融科技呈现出“破坏性创新”的突出特点，将会从金融监管法律、金融监管协同两方面冲击金融监管。

借鉴欧盟应对支付欺诈的改革方案，首先，建议我国发展明确监督科技应用的法律依据与政策引领，扎实让科技赋能监管机构与监管能力的顶层设计。尤其是在支付风控模型与风险控制策略方面，要积极运用大数据、人工智能等技术拓展事前风险信息获取、事中风险计量与模型研发，以及事后数字化补救与应对措施，推动支付反欺诈监管朝向“技防”“智防”转型。其次，从涉及欺诈的基础性数据领域，要实现结构化与非结构化数据有效整合，整合行内外和跨行业数据及多维度跨场景行为特征，提升监管机构的大数据处理技术。最后，加强与金融科技企业、大数据企业在信息共享、数据利用和技术采购等方面的合作，推广机器学习、跨平台数据引入、图计算技术与大数据分析等技术在监管层面的应用。N ①

学术编辑：韦燕春

EU Payment Anti-Fraud Regulatory Reform Centered on Information Sharing: Lessons for Reference

WANG Hanting SHANG Bowen

(School of Law, University of International Business and Economics)

Abstract As digital technology empowers the financial services market, payment fraud prevention has become increasingly critical to the high-quality development of China's finance in what is widely referred to as the "new era". The European Union has established a regulatory framework centered around its Payment Services Directive to standardize payment rules and boost consumer protection. But even a strong customer identity verification mechanism struggles to cope with the new problem of "impersonation fraud", and information leakage and regulatory consistency issues have become obstacles to anti-fraud supervision in the payment segment of the market. A new round of EU reform focuses on the construction of information monitoring mechanisms and consumer education. It also takes aim at the need for the timely sharing of fraud-related information by service providers and improved responses to fraud claims by consumers. A balance has been achieved between payment fraud prevention and consumer information protection, but there are flaws in the legal foundations of data processing that need to be addressed. China should make "information sharing" the center of its payment anti-fraud efforts, but it also needs to devote more attention to the construction of its legal system in regards to information sharing. Greater cooperation between domestic and foreign institutions is also essential in the regulatory sphere.

Keywords Financial Fraud, Payment Fraud, Fraud Regulation, Information Sharing, Information Protection

JEL Classification G18 K24 L86

① 参考文献[1]~[40]，见增强出版，中国知网—《金融市场研究》。