DOI 10.15302/J-SSCAE-2020.06.013

金融零售支付风险控制的现状、挑战与对策研究

周皓 [1, 2]，**柴洪峰** [1, 2, 3]

（1. 上海交通大学网络安全技术研究院，上海 200240；2. 中国银联股份有限公司，上海 200135；
3. 电子商务与电子支付国家工程实验室，上海 201201）

摘要：随着我国金融开放、普惠金融与金融科技的发展，金融零售支付产业正在由高速度增长向高质量增长转型升级，当前金融零售支付风险呈现出更加复杂严峻的态势。新型冠状病毒肺炎疫情的发生，使得人们的消费和支付习惯发生了很大变化，已经对金融零售支付风险控制研究提出了新的课题。本文分析了金融零售支付风险控制的新特点与不足，梳理了金融零售支付风险控制的现状，产业主体在合规履职、账户管理、交易监测、信用评估、数据安全、身份验证、技术风险等七方面的挑战。研究提出了关键在于建立完善与复杂严峻态势相匹配的全面风险管理体系与智能风控体系的观点，具体从数据共享、智能模型、系统架构、管理体制、人才培养五方面提出了对策建议。

关键词：金融零售支付；支付风险；风险控制；金融犯罪；金融智能

中图分类号：TP391　　**文献标识码：**A

Financial Retail Payment Risk Control: Current Status, Challenges, and Countermeasures

Zhou Hao [1, 2], **Chai Hongfeng** [1, 2, 3]

(1. Institute of Cyberspace Security Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China;
2. China UnionPay Co., Ltd., Shanghai 200135, China; 3. National Engineering Laboratory of
Electronic Commerce and Electronic Payment, Shanghai 201201, China)

Abstract: The development of financial openness, inclusive finance, and financial technologies in China is transforming and upgrading its financial retail payment industry from high-speed to high-quality growth; consequently, the risks for financial retail payment currently present a more complex and severe situation. The COVID-19 epidemic has changed people's consumption and payment habits and raised new topics on risk control of financial retail payment. This study explores the demand for risk control of financial retail payment in China by analyzing the new characteristics of financial retail payment and the deficiencies in the risk control. It then summarizes the current status of the risk control and the major challenges from seven aspects: compliance performance, account management, transaction monitoring, credit evaluation, data security, identity verification, and technical risks. We conclude that the establishment and improvement of a comprehensive risk management system and an intelligent risk control system that match the complex and severe situation is the key to financial retail payment risk control. Furthermore, we propose several countermeasures specifically from five aspects: data sharing, intelligent model, system design, management system, and talent training.

Keywords: financial retail payment; payment risks; risk control; financial crime; financial intelligence

收稿日期：2020-09-10；**修回日期：**2020-10-28

通讯作者：周皓，上海交通大学网络安全技术研究院高级工程师，研究方向为金融安全与风控技术；E-mail: zhouhao@unionpay.com

资助项目：中国工程院咨询项目“网络空间安全保障战略研究”(2017-XY-45)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

金融零售支付体系作为金融制度的基础安排，贯穿于金融活动的全过程，在金融体系中具有特殊的地位和作用，是支撑经济运行和社会发展的基础设施 [1]。中国人民银行《2019 年支付体系运行总体情况》显示，全国支付体系运行平稳，社会资金交易规模不断扩大，支付业务量保持稳步增长；金融零售支付业务量覆盖面较广，交易规模比重较大；2019 年，我国人均拥有银行账户数达 8.09 户，人均持有银行卡 6.03 张，支付系统共处理支付业务 5.685×10^{11} 笔，主要处理零售支付的银行卡跨行支付系统与网联清算平台合计占比为 93.7%。

随着金融科技的快速发展，金融零售支付业态深化变革，迎来了新的产业格局、发展模式、技术实现 [2]。在产业格局方面，产业参与方（指承担具体角色的一方）日益多样化，以移动支付为例，新增了移动设备厂商、应用程序（APP）服务方、聚合支付服务商、支付科技服务商等。在发展模式方面，商业银行强化移动端 APP 和“开放银行”建设，深化与互联网流量应用服务提供商的合作，扩大支付在消费金融等零售业务的发展；非银行支付机构借助支付通道附加提供综合商户服务方案，逐步拓展境外支付市场。在技术实现方面，支付载体从磁条卡到芯片卡、再到二维码，受理终端从传统销售终端（POS）到无线终端、再到手机 POS 机，通信方式从专线到互联网、再到物联网，身份认证从交易密码到短信验证码、再到指纹、人脸等生物特征，平台架构从集中式到分布式、再到区块链。

在金融零售支付业务快速增长、业态深刻变革、风险形势严峻的背景下，探讨保障我国金融零售支付业务健康发展的思路和措施具有迫切性。本文分析金融零售支付风险控制的需求（包括特点与难点），梳理金融零售支付风险控制发展现状；针对合规履职、账户管理、交易监测、信用评估、数据安全、身份验证、技术风险等方面的挑战，提出保障措施建议。

二、金融零售支付风险控制的需求分析

金融零售支付风险与创新发展始终相伴相随、交织前行，当前面临五方面的新特点：①新的参与方，除了传统商业银行、支付清算组织、非银行支付机构，还有移动手机终端厂商、互联网巨头企业、金融科技初创公司等，新的参与方可能引入新的风险；②新的业务形态，支付业务场景逐渐从到店支付演变为随时支付，支付不再是单一的活动，不断地渗透和融入到信贷、理财、保险、租赁等其他金融场景中，风险也从单一业务环节向全链条蔓延并扩散；③新的网络黑产 [3,4]，人工智能（AI）技术广泛应用于科技创新的同时，也被网络黑产组织所利用，犯罪手法有集团化、专业化、智能化、国际化演变的势头；④新的违法犯罪，受利益驱动，跨境赌博、电信网络诈骗、利用暗网与比特币洗钱等违法犯罪活动屡禁不止，从线下场景转移到线上场景，持续引发了国家层面的高度关注，多部门联合打击治理跨境赌博，依法处罚提供资金支付结算的平台机构；⑤新的矛盾焦点，《中华人民共和国网络安全法》发布、《中华人民共和国个人信息保护法（草案）》公开征求意见，使得个人信息保护与数据智能使用之间的平衡成为新的矛盾焦点，有利于促进用户隐私保护技术的研究与应用。

面对金融零售支付产业的深刻变革和严峻态势，支付风险控制尚存在四方面不足。①风险认知尚未完全适应风险快速演变的趋势，信用风险持续上扬，欺诈风险不断翻新，合规风险趋于严重，清算流动性风险开始显现；支付服务主体（指支付清算组织、商业银行、非银行支付机构）对前述风险危害的认知不一致，应对风险的控制体系能力也存在较大差异；②数据应用尚未完全弥补风控体系的短板，有关案件 [5] 表明，不法分子正是利用了风控机制、风控系统、风控模型方面的缺陷才得以实施欺诈或犯罪，然而关联数据由于未充分授权、未有效采集、未加工清洗、未交叉分析，导致难以实现事前及早提示、事中及时预警、事后尽快修复；③ AI 尚未完全适配智能风控的可解释性需求，神经网络等智能算法在医疗 [6]、交通 [7]、农业等领域的应用正在逐步进入商用，但是基于 AI 的风控模型体系建设还有待完善与验证，特别是算法的可解释性、个人隐私保护、公平建模等方面面临一定的挑战；④管理机制尚未完全符合治理体系的要求，建立完善的全面风险管理体系是金融企业治理现代化的重要环节，必然要求在企业内部加强全员风险意识，设置风险专业板块；不同机构内部的风

险管理组织架构还有待强化，风控理念还需要转变。

现阶段，金融零售支付领域风险控制愈发重要，已经成为支撑支付产业高质量发展的保障战略之一。亟需从数据共享协同、模型智能升级 [8,9]、系统集约统一、全面风险管理、交叉人才培养等方面着手，加快建设步伐，尽快形成有效应对不断变化风险态势的综合能力。

三、金融零售支付风险控制的发展现状

在用户需求的持续推动、金融科技的助力支撑下，金融零售支付产业链条不断延伸、创新发展，链条上的监管部门、服务主体、相关参与方（见图 1）更加关注风险控制的价值与意义：监管部门多措并举防范支付领域的高发风险；支付清算组织稳妥推进风险清理并着力提升风控服务水平，商业银行纷纷探索大数据和 AI 技术在银行风险监测中的应用，非银行支付机构按监管要求集中存管客户备付金；金融科技公司提供包括智能感知、智能分析、智能决策、智能处置的智能风控服务和产品。此外，支付服务主体更加关注个人信息保护，国际芯片卡标准化组织发布的支付标记化技术规范 [10] 在我国也取得了较好的应用效果。

（一）监管部门不断加强对支付风险控制的要求

近五年，中国人民银行、中国银行保险监督管理委员会一直加大防范化解金融风险的要求和处罚力度，对于违法违规的商业银行、非银行支付机构、相关从业机构依法处置，以遏制行业高发风险、维护金融市场秩序。

2015—2019 年，中国人民银行在“中国支付清算论坛”上分别提出把握监管和创新、平衡安全和效率、匹配开放与监管、严监管常态化、严控各类交叉风险等核心原则；同时指出，非银行支付机构不同于一般工商企业，必须加强风险控制、强化风险意识；建立有效的风险管理机制，推动行业风险信息管理系统建设；对存量风险采取既定的措施消化，对增量风险加强监测、“抓早抓小”、提前防范，处理好不同主体之间的风险，着眼于系统性风险防范；在电信网络诈骗、跨境赌博、网络黑灰产业、账户风险监测等方面，要求建立黑名单制度，持续完善风险监测水平。

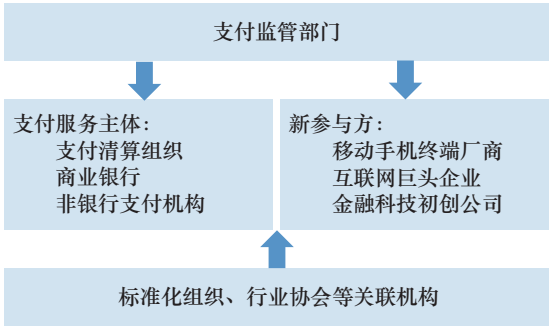

图 1　金融零售支付产业的主要参与方

（二）支付清算组织稳妥推进风险清理与提升风控服务水平

作为银行卡清算业务处理的枢纽，中国银联股份有限公司联合产业各方，积极开展 II、III类账户风险防范、备付金风险监测、打击电信网络诈骗和跨境赌博、支付风险安全检查、账户信息安全管理等风险整治工作，配合中国人民银行、公安部门研究解决“一人多卡”、自助取款机（ATM）生物识别等问题 [2]。

面对产业高发风险，中国银联股份有限公司及时开展机构约谈、高风险商户责任转移等约束处置工作，联合产业各方妥善处置了电子不停车收费系统（ETC）盗刷、境外集中欺诈、跨境移机等风险事件，通过实时监控、货物拦截、资金延迟结算机制，2019 年共为机构和持卡人避免（或挽回）损失约为 8.3 亿元。中国银联股份有限公司依托中国银联风险管理委员会、银行卡安全合作委员会、互联网支付安全联盟等基础平台和机制，加强沟通交流、深化产业合作、强化联防联控，保障持卡人合法权益。中国银联股份有限公司不断升级智能风控能力，建设一体化智能风控体系架构、机器学习建模平台，构建支付产业中跨单位、跨领域、跨条线的合法合规共享数据机制。中国银联股份有限公司推进覆盖基础风险控制、标准风控应用程序接口输出、定制化解决方案的三级风控产品体系，截至 2020 年第三季度，为超过 130 家金融机构与非银行支付机构提供了相关服务。

作为非银行支付机构与银行间网络支付业务处理的支付清算组织，网联清算有限公司通过机构及资金的异动监测等手段，持续为监管部门监控风险提供及时准确信息，实现风险隐患及时排查处置；

针对资金违规挪用、个人对个人（P2P）高危交易等风险场景，建立了市场主体资金异动监测分析和信息联动同步机制；基于智能学习技术，建立了涉嫌赌博交易等违规行为监测模型 [11]。

境外支付组织 Visa Inc. 和万事达国际组织也正在建立完善基于大数据的风险控制机制。例如，Visa Inc. 为银行等金融机构提供风险控制服务，通过识别交易主体身份与交易欺诈风险来提高交易安全性与处理效率；具体提供了银行卡交易授权管理、欺诈检测、基于生物特征的用户身份验证解决方案、基于发卡行授权交易数据预测逾期风险的个人信用评估等服务。

（三）商业银行提升支付风险精细化管理水平

不同类型的商业银行结合自身业务发展需要，均在风险控制方面加大科技与业务投入，特别是零售、普惠等业务板块，更是将支付风险控制放在重要位置。

国有银行建立了全行风控体系，如中国工商银行股份有限公司构建了“风险 + 智能”的智慧风控体系，部署超过 200 个实时计算和准实时计算模型，累计预警和阻断超过 2×10^7 笔信用卡、借记卡和电子银行欺诈交易，有效遏制各类欺诈行为 [12]。股份制银行建立了全流程风险管理体系，如招商银行股份有限公司建设智能化的大数据反欺诈平台，综合运用移动设备指纹、光学字符识别、人脸比对、电子合同比对等技术手段，显著提升风险管理水平和操作效率 [13]。各地区的城市商业银行、农村商业银行、农村合作银行、村镇银行、农村信用社、外资银行等，针对高风险领域建立了相应的风控系统和措施，如江苏银行股份有限公司构建了基于关联图谱的反欺诈体系 [14]。

（四）非银行支付机构风险频繁暴露

随着互联网经济的快速发展，非银行支付形成了很多新的业务模式，在带来机遇的同时也引发了问题，如外部监管风险、备付金管理风险、人为操作风险、网络犯罪风险、流动性风险、财务风险等 [15]。

《非银行支付机构客户备付金存管办法（征求意见稿）》对于挪用备付金的行为，明确按照《中华人民共和国中国人民银行法》进行处罚。2020 年 6 月，某非银行支付机构的母公司发布公告，与该非银行支付机构有业务关系的公司挪用其备付金账户资金 14.95 亿元，其支付牌照或将被吊销。2020 年 7 月，上海市人民检察院披露一起利用黑客技术侵入非银行支付机构计算机系统盗窃案，2018 年 4—6 月，犯罪分子利用上海某理财平台和 P2P 公司之间的充值系统漏洞，采用编造方法将小额实际充值虚增为巨额金额，再从备付金账户将上亿元巨额资金划转至 P2P 账户，进而非法占用。2020 年 4 月，某非银行支付机构的文件数字证书被黑客攻击，经查验，系黑客利用盗窃的文件证书伪造支付指令，短时间内向犯罪分子控制的多个账户累计支付资金上亿元。

（五）支付风控服务方提供专业化风控能力

在监管力度不断加大、支付业态加速变革的双重影响下，抵抗风险的能力可支持企业提质、增效、降本，成为产业各参与方认可和致力的方向。商业银行和非银行支付机构意识到自身的风险数据和风险模型存在不足，支付风控服务方也由此出现并发展。

境外支付组织 Visa Inc.、万事达国际组织在履行支付清算职责同时，也在风险责任分担体系框架下，通过分析交易网络内的可疑交易与异常信息，向成员机构提供了支付安全服务。大型互联网企业则以 10 亿个数量级别的用户数据为基石，输出其训练和孕育出的 AI 模型、画像分析技术能力。智能分析决策厂商凭借创新技术能力与金融服务经验，帮助客户部署本地化风控系统与模型。中国银联股份有限公司参照 Visa 和万事达的支付安全服务模式，结合我国支付风控服务市场需求，提供分层级、分类别、分客群的风险服务。

四、金融零售支付风险控制面临的挑战

（一）合规履职

中国人民银行、中国银行保险监督管理委员会更加关注全面风险管理，不断加大与公安部门联合打击犯罪活动的力度，运用现代科技手段强化支付市场合规风险监测，开展执法检查工作并加大处罚

力度。对标上述严格要求，部分支付服务主体存在制度体系不健全、风控系统不健壮、风险运营不到位等问题。以信用卡贷前审批制度体系为例，2014 年上海银保监局提出“刚性扣减”要求后，部分商业银行单纯追求业务发展目标而未按要求审批，对于收入未达要求的客户过度授信，2019 年受到行政处罚。2020 年 7 月发布的《商业银行互联网贷款管理暂行办法》，要求将互联网贷款业务纳入全面风险管理体系，确保互联网贷款业务发展与自身风险偏好、风险管理能力相适应。

（二）账户管理

在跨境赌博、电信网络诈骗、恶意套取营销资金等过程中，犯罪分子利用个别银行账户的管理缺陷与技术漏洞，有组织地集中申请个人账户或分散购买个人账户并用于资金转移，形成了实施犯罪的账户链与资金链。犯罪分子还利用个别银行在Ⅱ、Ⅲ类银行账户，企业银行账户远程开立验证方面的技术缺陷，批量进行验证与开户，远程实施犯罪活动。

（三）交易监测

犯罪团伙利用窃取的支付账户信息及短信验证码，在境外高危风险国家和商户进行恶意盗刷。随着移动支付的发展，犯罪团伙在盗取信息后先尝试虚假申请（即在手机 APP 中绑定支付账户）、再恶意盗刷，并且犯罪手法不断变化、趋于隐蔽，给传统的基于规则拦截或预警的方式带来了挑战。除了运用风险大数据开展用户行为分析 [16]、建立覆盖移动支付交易全流程的风险监测手段 [17] 以外，迫切需要提升风险态势感知与实时量化决策的监测能力，从防范犯罪个体拓展至防范黑产团伙。

（四）信用评估

受宏观经济下行、全球新型冠状病毒肺炎疫情的交叉影响，银行零售信贷与信用卡业务的不良贷款金额和比率不断上升，部分中小金融机构的信用风险问题较为严重。随着互联网金融贷款平台的整治与清理，低收入、高共债客户群体的低偿还能力成为银行信贷业务的输入性风险点，为此银行迫切需要加强共债人群的识别、区分、管控。部分银行开展了远程互联网贷款业务，但是尚未建立匹配的风险管理体系，特别是在风险模型和人工复核方面缺乏有效管理。

（五）数据安全

数据安全涉及支付信息泄露带来的挑战，又包括用户隐私保护对智能模型带来的挑战。支付信息泄露的方式发生了变化，从原先在 ATM 安装测录装置获取少量单点信息，到黑客攻击存有系统漏洞的商户或非银行支付机构系统获取批量多点信息，再到攻击手机 APP 获取全套信息并在互联网及暗网上出售，使得监测分析的难度加大；迫切需要通过基于互联网及暗网的风险情报分析、深层学习模型等智能计算技术来提高分析的覆盖面与准确性 [18,19]，变被动响应为主动预警。在数字化时代，数据成为企业驱动经营决策、提升运营效率的重要资产和战略资源，但受隐私保护与个人金融信息保护的法律法规要求，打破“数据孤岛”、平衡隐私保护与数据应用成为重要课题。

（六）身份验证

作为数字经济时代的信任基础之一，可信数字身份逐步被金融机构应用于身份识别、场景融合、风险控制、隐私保护等多项业务流程。公安部门以“互联网 +”可信身份认证平台核心技术为依托，建立了权威、安全、可信、便捷的网络身份认证体系，推出了居民身份证网上功能凭证，积极促进网络电子身份的国际互认 [20]。生物特征识别已经成为用户身份验证的重要因素，一旦发生泄漏并遭到非法使用，将严重损害用户自身利益。这对生物特征识别 AI 算法模型提出了挑战，如分辨用户意愿的真实性、从实人认证到实意认证。

（七）技术风险

科技成果在支付风险控制领域的不当应用，可能导致业务安全与技术风险的双重叠加，进而对支付市场、交易、产品产生更大的冲击 [21]。AI 已经在支付风险控制领域试点和应用，近期有学者针对 AI 安全问题、安全威胁展开了研究，认为技术缺陷、可解释性差可能会造成不可逆的安全威胁。算法和数据是 AI 的核心，都面临潜在的安全风险，会导

致 AI 应用决策的风险 [22]。此外，AI 系统在实际运行中也存在安全风险，一旦设计不当，容易被攻击者利用开展非法活动。

五、对策建议

（一）构建多层次的大数据共享、分析与反馈平台

从国家、行业、企业 3 个层面着手，构建多层次的大数据共享、分析与反馈平台，作为公共基础服务为金融零售支付服务主体提供重要支撑。

在遵循国家有关法律法规的前提下，建议由国家监管部门构建多部委联合的数据共享机制，参照打击跨境赌博、电信网络诈骗的部委联合工作机制，进一步充实完善国家级别黑名单基础库；在大数据征信领域，加快建设覆盖农村人群、互联网借贷信息的权威信息库。经国家有关部门批准，在地方政府的支持下，地方监管部门牵头筹建地区性的数据共享平台，推动当地政府部门、公共事业单位的征信类信息入库，打造具有地方特色的征信服务平台，服务本地金融机构。

支付行业协会与支付清算组织从防范支付风险、促进支付产业健康发展的角度出发，构建基于市场自愿规则的行业级别大数据分析体系。例如，中国银联股份有限公司利用自身网络内跨机构交易数据及风险案件处置能力，基于区块链、云计算技术，开展风险控制数据、情报的共享分析服务，建立联防联控机制。

支付服务主体是大数据风险控制应用的用户。建议按照中国人民银行关于建立大数据风险控制体系的要求，打通企业内部各业务条线的数据，在业务产品中获取用户的数据授权，构建一体化大数据管理与应用平台。对于接入、使用国家和行业大数据平台的，应按要求及时上报数据，反馈查询数据后的应用与决策结果，使得数据应用动态闭环。

（二）推进 AI 技术在风控领域的纵深应用

AI 技术在金融零售支付风险控制领域的应用尚处于起步阶段，仅一部分大型互联网企业、全国性银行、支付清算组织开展了探索与试点；更多的金融机构仍然依靠基于经验、基于规则的方式开展风险控制，或者仅在个别业务领域应用了机器学习算法。为满足支付及关联金融场景的高并发、实时性、低容忍的业务要求，建议尽快解决模型成熟度、数据可用性、算力可靠性等问题，促进 AI 应用的普及。

在模型成熟度方面，监管部门已经提出风险模型全生命周期管理流程及要求，AI 技术在风险模型方面的应用应补充相关技术规范和测试指南，支付服务主体需制定与应用场景相关的 AI 模型成熟度指标体系，科研院所和高校可配合开展金融实时风险控制场景下的高认知模型基础研究与技术攻关。

在数据可用性方面，风险控制所需的数据必然是海量数据，包括企业内部数据和外部数据。在个人信息保护法规与监管趋严的时代，迫切需要加快隐私保护技术的应用，如基于区块链、安全多方计算、联邦学习框架等技术的数据联合建模，双方不共享数据，但依然能够发挥数据融合的价值。

在算力可靠性方面，AI 模型运行、大数据分析均需要较强的硬件资源；支付服务主体应规划制定 AI 算力及支撑平台的技术路线图，扎实推进基础设施建设。

（三）提升风险控制系统的全面性与鲁棒性

风险控制系统与业务系统既耦合又分离，建议支付服务主体建立面向业务系统的集中智能风险控制系统。

关于全面性，建议打通数据、模型、策略、运营全环节。数据环节负责“原材料”，将不同业务条线的数据进行归类和处理，涵盖实时流式计算、准实时分发、批量标签预生成等。模型环节是“来料加工”，将多维数据导入算法规则体系，实现快速计算和形成量化结果。策略是“分类分级”，根据业务预期指标开展智能决策。运营是“触达客户”，自动化完成工作流所有事宜，提升客户体验，形成闭环。

关于鲁棒性，实时风控系统作为复杂系统工程，通常涉及当笔数据、历史标签、黑灰名单、外部数据、模型规则、监测策略、运营流程等多个模块；架构设计应充分评估业务增长、外部接口、系统安全、备份机制、熔断机制、系统性能等关键技术设计方案，确保低延迟、高并发、弹性化。

（四）倡导全面风险管理的文化与意识

建立完善的全面风险管理体系是金融企业治理

现代化的重要环节，建议在企业内部强化全员风险意识，设置风险专业板块或部门；从管控风险向经营风险转变，推动风险服务向嵌入式、一站式服务升级，实现对企业各个业务条线、所有风险种类和不同岗位人员的全覆盖。

支付产业当前面临的风险形势严峻，建议商业银行等支付服务主体建立完善全面的风险管理机制，构建风险中台；确定不同阶段的风险管理目标，开展风险管理评价及全流程管控，界定不同业务条线业务部门的风险职责，防范化解系统性风险。

（五）加大支付风险控制复合型人才培养

传统的风险控制专家都是业务领域的专家，专业背景通常是经济类、金融类专业，少量是统计、数据分析相关专业。随着大数据、AI、云计算等科技成果在风险控制领域的应用普及，复合型人才的需求变得尤为迫切。

建议高度重视并加快培养复合型人才队伍，在传统的风险控制专家之外，补充数学、计算机、网络空间安全等专业背景的人才；推动数据分析、AI、架构设计等能力与支付风险控制的业务需求相结合，打造理论基础扎实、实战经验丰富、管理能力完善的智能化风险控制专家团队。

参考文献

[1] 温信祥. 关于建设新时期现代化支付体系的思考——基于国家治理体系和治理能力现代化视角 [J]. 学术前沿, 2019 (24): 66–71.
Wen X X. On the establishment of a modern payment system in the new era—Based on modernizing China's system of governance and governance capacity [J]. Frontiers, 2019 (24): 66–71.

[2] 邵伏军, 时文朝. 中国银行卡产业发展报告 [M]. 上海: 上海文化出版社, 2020.
Shao F J, Shi W C. Report on the development of China's bankcard industry [M]. Shanghai: Shanghai Culture Press, 2020.

[3] 陈岳峰, 毛潇锋, 李裕宏, 等. AI安全——对抗样本技术综述与应用 [J]. 信息系安全研究, 2019, 5(11): 1000–1007.
Chen Y F, Mao X F, Li Y H, et al. AI security—Research and application on adversarial example [J]. Journal of Information Security Research, 2019, 5(11): 1000–1007.

[4] 朱丽芳. 人工智能技术在应用中的安全风险与管控研究 [J]. 电信工程技术与标准化, 2019, 32(12): 33–37.
Zhu L F. Research on artificial intelligence security problems and control measures [J]. Telecom Engineering Technics and Standardization, 2019, 32(12): 33–37.

[5] 赵斌, 柴洪峰. 打击银行卡犯罪精品案例集（2014—2016）[M]. 北京: 法律出版社, 2017.
Zhao B, Chai H F. A collection of excellent cases against bank card crimes (2014—2016) [M]. Beijing: Law Press · China, 2017.

[6] 陈新华, 蒋建文, 周华, 等. COVID-19疫情背景下的医院人工智能快速布局和发展战略探讨 [J]. 中国工程科学, 2020, 22(2): 130–137.
Chen X H, Jiang J W, Zhou H, et al. Rapid layout and development strategy of hospital artificial intelligence during the COVID-19 pandemic [J]. Strategic Study of CAE, 2020, 22(2): 130–137.

[7] 赵世佳, 徐可, 薛晓卿, 等. 智能网联汽车信息安全管理的实施对策 [J]. 中国工程科学, 2019, 21(3):108–113.
Zhao S J, Xu K, Xue X Q, et al. Implementation countermeasures for information security management of intelligent connected vehicles [J]. Strategic Study of CAE, 2019, 21(3): 108–113.

[8] Zheng X L, Zhu M Y, Li Q B, et al. FinBrain: When finance meets AI 2.0 [J]. Frontiers of Information Technology & Electronic Engineering, 2019, 20(7): 914–924.

[9] Pan Y H. Heading toward Artificial Intelligence 2.0 [J]. Engineering, 2016, 2(4): 409–413.

[10] EMVCo. Payment tokenisation specification technical framework V2.1 [EB/OL]. (2019-06-14)[2020-08-20]. https://www.emvco.com/emv-technologies/payment-tokenisation/.

[11] 董俊峰. 高效支付保障金融安全 [J]. 中国金融, 2019 (21): 40–42.
Dong J F. Efficient payment guarantees financial security [J]. China Finance, 2019 (21): 40–42.

[12] 张艳. 夯实安全防护基础 构建攻防兼备安全体系 [J]. 中国金融电脑, 2019 (8): 9–13.
Zhang Y. Consolidate the foundation of safety protection and build a safety system with both offensive and defensive functions [J]. Financial Computer of China, 2019 (8): 10–13.

[13] 郑岩. 科技如何支撑"数字化转型" [J]. 金融电子化, 2018 (4): 24–28.
Zheng Y. How technology supports "digital transformation" [J]. E-Finance, 2018 (4): 24–28.

[14] 徐劲, 乔辉. 关联关系图谱, 欺诈风险防范新工具 [J]. 金融电子化, 2020 (6): 94–95.
Xu J, Qiao H. Association graph, a new tool for fraud risk prevention [J]. E-Finance, 2020 (6): 94–95.

[15] 张琳. 我国第三方支付的风险分析与防控控制研究 [J]. 智库时代, 2020, 228(8): 38–40.
Zhng L. Research on risk analysis and prevention of third party payment in China [J]. Think Tank Era, 2020, 228(8): 38–40.

[16] 柴洪峰. 互联网时代的银行卡产业风险防控研究 [J]. 中国信用卡, 2016 (6): 38–41.
Chai H F. Research on bankcard industry risk prevention and control in the era of Internet [J]. China Credit Card, 2016 (6): 38–41.

[17] Zhou Y K, Chai H F. Research and practice on system engineering management of a mobile payment project [J]. Front of Engineering Management, 2017, 4(2): 127–137.

[18] 杨善林, 周斌, 贾焰, 等. 网络舆情监测、分析与管理的现状与挑战 [J]. 中国工程科学, 2016, 18(6):17–22.
Yang S L, Zhou B, Jia Y, et al. On the monitoring, analysis, and management of network public opinion: Current status and

challenges [J]. Strategic Study of CAE, 2016, 18(6): 17–22.

[19] 李建华. 网络空间威胁情报感知、共享与分析技术综述 [J]. 网络与信息安全学报, 2016, 2(2): 16–29.
Li J H. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space [J]. Chinese Journal of Network and Information Security, 2016, 2(2): 16–29.

[20] 方滨兴, 杜阿宁, 张熙, 等. 国家网络空间安全国际战略研究 [J]. 中国工程科学, 2016, 18(6): 13–16.
Fang B X, Du A N, Zhang X, et al. Research on the international strategy for national cyberspace security [J]. Strategic Study of CAE, 2016, 18(6): 13–16.

[21] 陈红, 郭亮. 金融科技风险产生缘由、负面效应及其防范体系构建 [J]. 改革, 2020, 313(3): 63–73.
Chen H, Guo L. The causes, negative effects and the construction of prevention system of financial science and technology risks [J]. Reform, 2020, 313(3): 63–73.

[22] 李建华. 人工智能与网络空间安全 [J]. 中国信息安全, 2019 (7): 32–34.
Li J H. AI and cyberspace security [J]. China Information Security, 2019 (7): 32–34.