互联网金融支付产业
安全联盟

数字支付时代安全白皮书

Security White Paper in the Digital Payment Era

2020

互联网金融支付产业安全联盟

二〇二〇年十一月

目 录

前　言

近年来，在大数据、人工智能、机器学习等新兴技术的发展及推动下，商业银行、支付机构及银行卡清算组织等各类支付业务主体正快速向移动支付、数字支付转型，与此同时，各种新的风险形态亦不断出现。2020 年新冠疫情的突然来袭，对支付行业发展运行模式产生了较大影响，产业各方面临的风险形势和安全挑战愈加严峻和复杂。联盟秘书处牵头起草编写了本白皮书，旨在记录支付行业数字转型升级的沿革，总结分析数字支付时代下支付业务参与机构面临的各类风险特点及形成原因，推动各参与方在健全监管法规、推动行业规范、强化产业协作等方面通力合作，共同提升行业应对新业态风险的能力，构建安全支付新生态。感谢联盟各委员单位提供的宝贵意见及建议，特别感谢工商银行、平安银行、银联商务等成员单位给予的大力支持。

一、背景

（一）支付产业背景

1.我国首张银行卡的诞生与银行卡联网通用

1979 年，随着国家改革开放，我国银行卡产业开启了发展之路。1985 年 3 月，中国银行珠海分行发行国内第一张银行卡，银行卡产业发展迈出实质性一步。2002 年，国内第一家银行卡组织——中国银联成立，标志着产业开始向集约化、规模化发展，进入全面、快速发展新阶段，银行卡时代扑面而来，银行卡发卡数量持续快速增长。截至 2019 年底，银联卡发卡数量已达 85.5 亿张。同时，银行卡受理环境持续改善，联网商户已达 2362.96 万户，联网 POS 机具 3089.28 万台，ATM 机具 109.77 万台。与此同时，我国银行卡产业主动拓展国际化道路，特别是近年来结合“一带一路”等发展机遇取得了长足进展，人民币银行卡全球受理网络已扩展到 179 个国家和地区，并在 61 个国家和地区发卡，银行卡联网通用实现了高速发展。

2.数字支付的兴起与发展

在信息技术推动下，基于计算机、手机、智能终端等支付载体，借助互联网、移动通信网络等支付渠道的数字支付应运而生。商业银行、非银行支付机构以及卡组织等支付业务参与方纷纷发力网络支付、APP 支付、条码支付等新兴支付业务。在各类数字支付快速渗透普及的同时，智能终端、手机 POS 等受理终端设备不断推陈出新，智能手表、手环等可穿戴支付设备陆续涌现，人脸、声纹、指纹、静脉等生物特征支付也逐步从实验室走向人们的生活。在人民银行“移动支付便民示范工程”统筹推进下，数字支付产业在医疗、教育、交通、公共事业等便民惠民领域进一步深化发展，中国已成为移动支付普及、应用范围最广、程度最深的国家。

3.数字支付的未来

近年来，随着金融科技创新方兴未艾，移动互联网、人工智能、大数据、云计算、区块链、物联网等信息技术与数字支付业务深度融合，从支付产品、业务流程、身份认证、精准营销、风险防控、客户服务等环节入手，支付场景不断从广度向深度延伸，支付科技也成为金融科技最活跃的部分之一，正在深刻重塑人们的消费行为和习惯，也必将为中国数字支付产业发展打开新的维度。展望未来，伴随着人民银行数字货币 DC/EP 在深圳、苏州的试点，新兴技术将成为产业各方转型升级的关键驱动力，推动数字支付产业向场景化、智能化、虚拟化方向创新发展，并引领数字支付安全防控不断迈上新台阶。

（二）政策监管形势

近年来，中国人民银行等监管机构坚持“支付为民”理念，保持严监管常态化一以贯之，大力开展防范和化解重大金融风险隐患工作，坚持“规范发展与鼓励创新”并重，陆续出台了多项监管政策，促进数字支付业务高质量发展。

1.加强支付信息安全源头治理，夯实数字支付体系的安全基础

支付数字化转型过程中，支付信息泄露事件屡有发生，并成为电信诈骗、非面和移动支付欺诈等风险的源头。对此，监管机构先后发布加强银行卡信息安全管理等要求的政策文件，并组织行业开展银行卡信息泄露风险和支付安全风险专项排查，要求强化敏感信息内控管理和安全防控，全面应用支付标记化技术，采用多因素身份认证方式直接鉴别客户身份，采取交易验证强度与交易额度相匹配的技术措施，从技术要求和安全管理等角度全面夯实数字支付信息安全基础。

2.明确数字支付体系下各主体分类，推动业务回归本位健康发展

随着数字支付的业务产品形态变革，支付链条不断延展，支付参与主体也不断增多。对此，监管机构厘清商业银行、银行卡组织、转接清算机构等各类主体的角色分工，明确支付机构不可变相从事转接清算业务；对收单外包机构提出了

风险管理要求，明确不得从事商户风险监测等核心业务，不得采集、留存特约商户和消费者的敏感信息；对移动金融客户端应用软件从风险防控、信息保护、实名备案、监督处置等方面也提出了安全管理要求和规范。监管政策多管齐下，推动数字支付产业走上主体分类明确、各方回归本位的健康发展轨道。

3.构建多层次账户应用体系，配套明确风险管理工作要求

数字支付创新产品的不断涌现和支付机构的跨界展业，推动了账户体系的多元化，各类账户在支付领域不断渗透。对此，监管机构将个人支付账户划分为三类，对银行账户也划分为 I、II、III 类，明确了 II、III 类个人银行账户的开立、使用、变更、撤销以及账户信息验证机制的相关细则；同时，要求加强 II、III 类账户风险管理，全面排查相关账户开户风险隐患，从账户开立和交易环节加强风险监测，并进一步明确开户环节身份信息联网核查及账户信息验证等业务管理要求，保障账户体系安全和客户合法权益。

4.打击治理涉赌、电诈等突出风险，保障人民群众的资金安全

数字支付在增强支付便捷性的同时，也由于其业态特性，使得相关支付接口易被网络赌博、电信诈骗等非法交易资金利用，成为快速汇集转移的重要通道。对此，监管机构明确要求加强支付结算管理，健全紧急止付和快速冻结机制，规范账户实名制及转账交易管理，强化特约商户与受理终端管控，开展防赌防诈提示和集中宣传，全力打击为跨境赌博、电信网络诈骗等违法违规活动提供支付结算服务的行为，坚决切断违法违规活动资金链，保障数字支付业态下人民群众的资金安全。

5.持续强化反洗钱合规管理工作，细化数字支付反洗钱管理要求

在数字支付业态下，洗钱资金流转链条越发隐蔽，而交易场景信息不透明、资金流向难以追踪等业务特性也都给反洗钱工作带来了新的挑战。对此，监管机构落实风险为本方法，不断明确对于客户身份核实、高风险领域管理、

跨境汇款业务管理、预付卡代销机构管理、交易记录保存和可疑交易报告等方面的要求。其中，细化规范了业务机构受益所有人身份识别、大额交易和可疑交易报告等方面的工作要求，还通过指引等形式明确洗钱和恐怖融资风险管理、反洗钱交易监测标准建设等方面的操作规范，全面提升反洗钱工作效果。

（三）产业发展动向

1.产业发展现状

（1）支付模式由卡基支付向账基支付升级演变

随着二维码和 NFC 近场支付等移动支付技术的日益成熟发展，用户的支付方式已从原有实体银行卡线下 POS 支付，逐步向手机、可穿戴设备等移动支付形态转变，持卡人应用移动端账户作为支付主体的特征日益显著；同时伴随着各类多元化主体的加入，以及支付标记化技术的推行，支付主体由银行卡向单位银行账户、非银行账户快速演变。

（2）支付场景从线下向线上迁移不断加速

近年来，交易从线下向线上迁移速度加快，产业各方也更加重视移动支付 APP，不断加大资源投入，持续完善 APP 功能。根据人民银行 2019 年支付体系运行数据，网络支付、移动支付业务交易笔数同比分别增长 37.14%和 67.57%，移动支付类头部 APP 注册用户数量稳步上升。

（3）支付产业参与者日益多样，产业合作日益紧密

随着人工智能、物联网、区块链等新兴技术在支付领域的应用日渐广泛，相关的智能算法、硬件、云服务、区块链平台等产品和服务提供方也加入到支付产业生态链当中。刷脸付、无感支付、无人便利店等新型智能支付场景被越来越多的用户接受和认可，相关生物特征识别、图像识别、智能硬件等厂商也逐步成为数字支付时代产业的重要参与者，进一步提升了支付业务的产品体验及安全性。商业银行、支付机构、卡组织等传统支付业务参与方与手机厂商、电信运营商等

新兴支付产业方的合作日益密切。多元化的支付产业模式需要明确各合作参与方的义务与职责，共同构建合作共赢的产业生态。

2.新兴支付形态

（1）人脸识别“刷脸”支付

2019 年是人脸识别技术应用于支付领域的元年，中国银联、支付宝和微信支付纷纷推出相应产品。其中，银联携手各大商业银行共同推出“刷脸付”，目前北京、上海、宁波、嘉兴（乌镇）等地均已正式上线，覆盖商超、餐饮、药店、酒店、自助售货机等众多便民场景。支付宝和微信支付分别推出“蜻蜓”第二代终端和“青蛙 Pro”等刷脸支付终端，并通过各种方式进行大规模市场推广。除人脸外，声纹、虹膜等生物特性信息也被用于替代传统账户身份验证方式，为用户提供更便捷、高效的支付体验。

（2）无感支付

无感支付是通过车牌识别、ETC、车辆 VIN 识别等多种方式，建立车辆信息与支付账户之间的绑定关系。开通无感支付服务后，持卡人无需主动发起支付动作，即可在指定商户自动扣款。目前，各类无感支付产品已广泛应用于停车场、高速收费、加油等出行场景，既提高了商户的经营运转效率，也为持卡人出行提供了更多便利与支付安全。

（3）支付标记化

近年来，维萨、万事达及银联等主要卡组织均相继推出了支付标记化（以下简称 Token）服务产品体系，Token 技术已广泛应用于支付领域。Token2.0 的升级发布，更是为支付产业的创新发展提供了生命力，赋予 Token 派生和 Token 集中管控两项重要功能。**Token 派生功能**，即通过已有 Token 申请新 Token，可以帮助用户实现“一次绑卡、处处使用”，通过 Token 推送或拉取的方式，帮助用户实现“快捷绑卡”，安全便捷地授权银行卡在不同场景进行支付。**Token 集中管**

控功能，即以钱包 APP 作为数字账户管理方，客户可以对 Token 生命周期进行集中管控和支付权限控制，自主掌控支付账户在不同支付场景下的限额、频次等权限。Token 技术将成为数字支付时代的基础核心要素，推动数字支付网络的不断优化升级，带来更安全、更便捷、更领先的支付体验。目前，中国银联已组织中行、光大等 7 家银行以及京东、美团等 5 家商户开展人民银行总行金融科技试点，实现手机银行 Token 推送、集中管控和快捷支付，并相继应用于快捷绑卡、心意卡券等业务场景。

（4）无号码银行卡

无号码银行卡是指实体银行卡上不显示银行卡号及其他涉及个人隐私或卡片信息（如：CVN2、有效期、持卡人签名栏等）的银行卡。该类银行卡实际也存在具体卡号，用户可通过银行 APP 进行查询。2019 年，苹果和 Grab 公司分别推出无号码信用卡 Apple Card 和 Grab Pay Card。2020 年 3 月，银联联合商业银行推出“银联无界卡”，采用线上虚拟卡+线下实体卡的形式发行，涵盖借记卡及信用卡产品。其中，信用卡具备消费功能，借记卡产品具备存款、购买投资理财产品等功能。同时，依托 Token 2.0 技术，“银联无界卡”可实现在不同绑卡场景分配不同 Token 并限特定场景使用，进一步保障用户的支付信息安全。

二、数字支付时代风险形势

（一）总体风险状况

近年来，支付市场开放稳步推进，支付基础设施不断优化，产业依托金融科技向多元化、数字化转型升级的步伐进一步加快，境外业务模式不断拓展，移动支付持续发展创新，支付产业进入了“深耕场景、共享资源，技术融合”的新时期。与此同时，受宏观经济下行、监管政策从紧、业态发展变革以及新冠肺炎疫情蔓延等诸多不确定性因素影响，支付业务风险隐患仍需高度警惕。

信用风险受疫情、共债和催收多重压力影响，风险持续攀升，资产质量管控压力与日俱增。与此同时，受信贷紧缩影响，专业化、团伙化的套现套利活动不

断滋生，并呈现线上线下套现同步发酵、从非金机构向商业银行蔓延等特征。

欺诈风险快速向线上移动端和创新支付产品聚集，并从交易层面向开户、验证、还款、交易、授信、转账全链条全方位渗透延展。同时，跨境风险加速凸显，受境外验证强度较弱、静态收款码跨境传播等因素影响，境外非面渠道欺诈大幅上升。

合规风险在机构间流窜隐匿并向 B 端业务迁移，部分机构商户资质审核不严、客户身份识别不健全、通道违规外放、包装改造交易场景，使得支付接口被利用作为电信网络诈骗、跨境网络赌博、洗钱等非法资金快速汇集转移的重要通道。

清算风险整体平稳但仍存隐忧，中小机构流动性风险问题不断凸显，个别支付机构挪用客户备付金、T0 垫资业务缺乏真实交易背景引发流动性危机等风险事件接连发生，给清算风险防控工作敲响了警钟。

此外，伴随着数字支付的快速发展，支付产品与服务持续创新，消费者权益保护工作还有待进一步提升完善：**一是**消费者自身在风险防范意识和能力等方面存在一定短板；**二是**部分机构消费者权益保护意识不足，使得消费者知情权、公平交易权与自主选择权等权益受侵害事件不断发生；**三是**犯罪手法更趋专业化、智能化、团伙化，消费者个人信息泄露事件时有发生，个人财产安全更易遭到侵犯。

综合分析上述风险形势的变化和特点，可以看出支付风险呈现以下新的发展变化趋势：一是风险从传统的线下渠道快速向移动互联网渠道和境外迁移；**二是**风险从资金交易环节向业务全链条全方位渗透，银行类 APP 也已成为欺诈分子轮番攻击的对象；**三是**风险类型从以欺诈风险为主向各类风险交织并存发展，尤其是合规风险日趋凸显，非法交易在各类支付场景之间隐匿逃窜；**四是**犯罪形态从个体作坊式攻击向集团化、专业化、智能化和国际化犯罪演变，防范系统性风

险压力进一步加大；**五是**风险产生的原因从业务产品为主向产品、人员及系统等多因素组合转变，系统安全与道德风险越来越需要引起关注；**六是**数据隐私安全和智能风控应用的矛盾开始显现，风险防控及外部合作将会迎来新的挑战。

（二）主要风险特征

1.经济下行压力加大，行业进入调整周期，信用风险积蓄攀升

（1）新冠疫情影响经济发展，行业扩张阶段风险进入暴露期

2020 年，突如其来的新冠疫情肆虐全球，不仅给我国经济发展带来强烈冲击，也严重影响了世界经济的运行趋势，导致经济压力由外向内传导，我国经济发展面临新的困难和挑战。特别是实体企业、外向型企业，经营利润下降、资产质量恶化，企业经营风险有进一步向个人传导的趋势，从业者工作和收入稳定性下降，影响消费及信贷偿付能力。

同时，银行卡授信规模保持稳步增长[1]，截至 2019 年底，银行卡授信总额达 17.37 万亿元，同比增长 12.78%。信用卡高速发展扩张阶段的审核简单、放款门槛低、重复授信等问题将在经济下行的压力下逐步暴露，行业整体信用风险呈上升趋势。

（2）互金风险加速出清，多头共债违约风险仍将进一步释放

互联网金融某些业态偏离正确创新方向，“714 高炮[2]”、暴力催收等问题时有发生，近期，爱钱进、网利宝等多家 P2P 平台，以及雪山贷、诸葛理财、铜掌柜等数十家违规网贷平台纷纷暴雷、跑路，行业规模大幅度收缩，平台风险迅速通过共债客户传导至银行信用卡业务，加剧了共债客群违约还款风险的释放和传导。

（3）社会资金紧缺导致套现套利更趋活跃，数字支付新业态下新型套现套利行为不断滋生

[1] 数据来源：中国人民银行《2019 年支付体系运行总体情况》和银保监会《2019 年银行业保险业主要监管指标数据情况》

[2] “714 高炮”是一种超高息的短期借款，分别为 7 天、14 天之内的。“高炮”是指其高额的“砍头息”及“逾期费用”。

近期，部分企业及个人收入下滑，社会资金紧缺，套现套利规模也逐步上升，新型案件不断涌现。“智能代还”是当前具有典型代表特点的套现行为，其利用信用卡账单日和还款日的时间差，获取持卡人卡片信息后，通过后台系统自动发起虚构交易进行套现和还款，以较小的金额进行循环还款。部分代还平台还使用“资金池模式”，一旦平台的资金池出了任何问题，或者平台携款跑路，持卡人的资金很可能血本无归。2020 年以来，代还 APP 专业化、产业化运营日趋明显，收单侧虚构商户、变造交易等行为使得风险侦测难度加大，对此类 APP 的打击关停，又使得相关用户资金链断裂，信用卡逾期风险快速上升，风险防控与处置面临两难境地。

此外，部分业务机构为迅速扩大市场份额，各类补贴、红包、抽奖等花式获客拉新方式层出不穷，催生了以“薅羊毛”为生的新型产业链。上游的卡商和黑客，负责提供大量手机号以及批量操作软件；中游的刷客搜集优惠信息、寻找规则或系统平台漏洞，利用手机号和软件抢夺各类优惠；下游的销赃团队专门负责将各类奖品和优惠变现，作案手法呈现智能化、团伙化、专业化等趋势。规模化“羊毛党”的存在，不仅严重扰乱了机构客户管理和营销推广，增加经营成本，还大幅侵占正常用户享受补贴优惠的权利。

（4）客户投诉、黑产攻击等事件频发，催收压力与日俱增

在经济下行、黑产攻击等因素影响下，贷后催收面临更大的压力和挑战。受网贷行业暴力催收曝光影响及整治连带效应，公众对催收业务负面情绪持续上升，加之疫情影响客户还款能力下降，催收矛盾更易激化，客诉压力不断增加。“反催收联盟”等黑灰产业规模化、专业化、产业化运营的特点更趋明显，甚至通过违规违法手段购买逾期人员名单主动、精准获客，对正常催收业务的干扰不断加大。

2.创新业务屡遭精准攻击，诈骗手法升级演变，欺诈风险持续暴露

（1）账基支付背景下风险向开户、交易等多环节传导，并跨机构、跨网络蔓延

数字支付时代下，随着支付模式向移动端快速迁移，对支付者的身份核身方式也由传统面对面核身，向非面核身转移，并渗透到开户、交易等多个业务环节，相应风险也由交易向开户等其他环节传导。2018 年以来，欺诈分子利用Ⅱ、Ⅲ类个人银行账户非面对面开户和跨行鉴权的特点，以及部分银行鉴权流程的缺陷漏洞，轮番发动欺诈攻击，在上下游银行间连环开户，最终伪冒开立的Ⅱ、Ⅲ类账户数量巨大，涉及银行较多，风险快速在机构及支付网络间蔓延。

（2）二维码、标签支付等新兴业务受理终端成本大幅下降，小微商户管理风险突显

近年来无卡支付、二维码支付、碰一碰支付等新型支付形态快速兴起，通过已有移动设备、纸质二维码或 NFC 标签等即可完成支付，其受理终端相比传统银行卡受理机具成本大幅下降，具有易获取、易传播等特性。同时，商户准入门槛低，使得受理市场管理难度大幅增加，规模化虚假、变造商户层出不穷，交易套冒绕形势严峻，产业各方在商户及交易终端风险管理和交易监测上面临新的挑战。

（3）新型电信诈骗案件层出不穷，犯罪团伙向专业化、产业化、跨国化发展

自去年以来，以“套路贷”、“杀猪盘”等为代表的新型电信诈骗发展迅猛，犯罪分子多从非法违规渠道获取受害人信息后进行精准诈骗，作案手法由骗取手机短信动态验证码后实施盗用，向主动诱导受害人发起资金转移转变。近期，以发放贷款需交纳手续费、保证金，以及疫情相关的代购口罩、爱心捐赠等话术的电信诈骗案件高发。公安机关侦破的相关案件中，非法团伙往往一次性获取数十万条贷款申请人的个人信息，并出售给电信网络诈骗分子，受害人近万名，涉案金额达数亿元。同时，不法分子多利用代理 IP、分身软件、群控设备、短信嗅探

等新型工具，诈骗区域由境内向境外及边境地区转移，作案专业化、产业化、跨国化特征日趋明显，风险管控与侦测难度日益加大。

（4）信息泄露助推境外风险上升，非面交易场景或成风险洼地

近年来，木马病毒、系统攻击造成的个人信息泄露事件频发，同时，境外支付产品由于验证强度普遍低于境内，且部分场景下仅凭静态信息即可完成交易，逐渐成为不法分子利用境内持卡人信息变现的主要目标。前期，代还 APP 引发了批量卡面信息泄露，部分已在境外发起欺诈交易。另外，由于静态二维码极易通过网络传播，跨境移码实施盗用的案件也时有发生。

3.市场环境愈加复杂、经营压力不断加大，合规风险日趋严重

（1）支付通道内非法交易风险频现，跑分平台等新型作案工具对风险侦测形成挑战

网络支付、移动支付等数字支付模式快速发展，在提升用户支付便捷性的同时，也滋生了部分非法或处于监管灰色地带的业务。尤其在疫情期间，线下赌博场景受到限制，客观上刺激了网络赌博规模增长。在经济下行的环境下，虚拟货币、非法贵金属交易平台则打着高收益的幌子吸引公众投资，非法行为屡禁不止，支付通道内违规交易风险频现。

为逃避监管和公安打击，并规避产业机构交易风险监控，网络赌博、虚拟货币等非法平台开始利用“跑分平台”等新型工具进行资金转移。跑分平台招募大量第三方支付真实用户，以抢单和分润的方式，雇佣其辅助赌博平台进行收付款。由于资金分散至多个真实账户，涉及账户数量较大，且大多账户原本为风控模型中的“可信账户”，风险侦测识别及处置账户难度大幅增加。对于跑分平台这一新出现的手法，相关法规和账户管理措施还不够完善，参与者也对行为后果没有清晰的认知，导致其体量快速增长，对风险防控提出了新的挑战。

（2）洗钱手法不断翻新变化，资金监测和调查难度持续加大

数字支付时代移动互联网的迅速普及以及支付产品形态的快速演变发展，为洗钱犯罪形式和手法带来了更多的可能性。犯罪分子借助互联网科技，在新兴行业领域不断延伸产业链，变换洗钱方式，洗钱案件呈现复杂化、多样化、隐蔽化及专业化等特点：

一是新兴经济领域洗钱风险快速集聚。互联网金融行业已成为洗钱犯罪重灾区，非法金融活动、“套路贷”、非法传销等新型经济犯罪手法不断翻新变化，规模屡创新高，严重扰乱了社会经济秩序。

二是新型支付方式洗钱风险持续攀升。以移动互联网支付、二维码与无卡支付等为代表的新型支付方式，具有交易便捷性高、业务参与方多、难以核实账户实际控制人等特点。通过上述支付方式转移资金，由于银行、收单机构均无法掌握完整、准确的交易信息，难以追踪分析和关联上、下游可疑交易和主体，加大了风险监测和调查难度。

三是犯罪分子尝试利用新型银行账户开展洗钱活动。银行账户虚假开立、非法买卖等是洗钱案件的常见行为，近年来，由于 II、III 类银行账户放宽开户要求，可通过非面渠道开立，已发生了犯罪分子集中批量开立 II、III 类账户的新型风险。尽管目前伪冒开立及买卖的账户主要出现在营销套利等场景，但后续被用于洗钱等违规业务的风险不容忽视。

（3）机构经营压力驱使违规操作屡禁不止，备付金业务衍生风险值得警惕

随着监管对于备付金的监督不断加强，支付机构合规管理意识逐步增强，但受到宏观经济复苏的不确定性以及支付市场日益加剧的竞争影响，仍然需要关注以下风险：

一是在经营压力驱动下，支付机构挪用备付金的利益冲动仍然存在。备付金集中存管后，支付机构通过备付金息差获取利润的商业模式不复存在，加上疫情影响，部分支付机构交易量大幅下降，个别机构的母公司甚至爆出破产的负面舆

情。支付机构自身或关联公司经营状况不佳，试图挪用客户备付金弥补亏空。

二是备付金业务中引发的合规风险值得警惕。个别支付机构疑似存在借用备付金业务为信用卡代还、P2P 商户等提供支付通道与资金结算服务，易由于违规业务受到打击而影响备付金业务正常开展。

（4）收单市场合规问题屡禁屡犯，行业整体风险防控压力加大

收单市场竞争加剧、互联网巨头挤压导致收单机构经营压力进一步增大，部分收单机构铤而走险，逐利而行，一再发生商户资质审核不严、核心业务外包、通道违规外放、受理终端管理不善、交易场景及商户类别变造等违规问题。

伴随着二维码等支付方式的兴起，受理成本急剧降低，商户入网门槛显著下降，收单机构核心业务外包使得聚合支付服务商成为银行、支付机构开拓下沉市场的重要合作方，收单机构对商户的实际掌控力严重不足。个别聚合支付服务商掌握大量商户池资源，并使用空壳公司、虚假商户进行交易包装、整合、拆分，掩盖真实交易场景和信息，并随意在机构、业务、产品间进行交易切换，导致业务风险快速规模化转移，严重干扰了发卡机构、卡组织等其他业务参与方的风险监控。同时，商户池业务模式往往伴随着优惠费率套用，涉嫌从事“二清”等监管机构严禁涉足的业务场景，对行业整体风险防范和打击处置带来严峻挑战。

4.机构核心系统仍存安全隐患，操作风险、清算风险稳中存忧

近期个别支付机构的在网络安全、内控管理、交易对账、应急处置等方面暴露出的一系列安全问题，反映出机构风险防控意识及能力相对薄弱，存在操作、清算风险隐患。

在经济下行、疫情影响和监管整治加强的形势下，一方面，应对个别以违规套现等为主营业务机构的经营风险引起高度关注，严防因其亏损、倒闭、跑路、牌照吊销等情形导致的后续交易清算风险；另一方面，近年来中小银行的数量不断增长，其在经济下行周期的抗风险能力相对较弱，已发生了多起银行利润滑坡、

出现严重经营问题的风险事件，其经营不善导致的清算流动性风险值得警惕。

5.黑灰产、暗网规模快速扩张，信息泄露风险成疾

在我国数字经济迅猛增长的态势下，依赖互联网生存的黑灰色产业链条向专业化、产业化形态快速转变，包括非法买卖银行账户、电话卡、身份证号，提供电信诈骗短信发送服务，搭建钓鱼网站等在内的一系列网络违法犯罪行为屡见不鲜，已形成价值庞大且盘根错节的利益链，并受多种因素影响，规模快速扩张：

随着黑客技术标准化及黑产工具愈发普及，参与者门槛不断降低，不法分子可以根据网站及论坛上的学习教程及标准化工具快速学习上手；网络诈骗、精准营销、引流变现等黑产市场需求日益扩大，产业链愈发复杂；交易日渐隐秘，黑灰产业的高暴利性引导参与者将交易转至暗网，加大了监管难度。

黑灰产规模的快速增长，导致网络攻击、撞库等信息系统安全和泄露事件频发，泄露渠道由单个泄露源向境内境外、多个终端及系统转变，涉及主体也由单个商户转移至收单机构支付系统、外围合作机构业务平台、跨行业 APP、违规类 APP 等外围参与方，特别近期代还 APP 平台违规留存用户敏感信息导致的信息泄露呈大规模、高频度趋势，APP 的信息安全或将成为新的防护重点。

（三）典型风险案例

案例一：“杀猪盘”诈骗

2018 年年底以来，通过社交软件、婚恋平台假冒所谓“高富帅”男性对单身女性实施诈骗的案件频发。犯罪分子先以谈恋爱为名与受害人交往，博得好感及信任后再伺机向对方“透露”自己在博彩网站上购买彩票，有内幕消息可以一起中奖发财，诈骗受害人投入巨额资金。此类诈骗手法俗称“杀猪盘”。

警方破获相关案件后，犯罪分子交代通过在境外购买服务器，建立赌博网站，开设赛车等多种博彩下注玩法，并高频度变换 APP 名称躲避打击。同时，通过招募大量业务员，统一购买社交软件账号、手机电话卡，培训话术，利用虚拟定位

软件在国内知名交友、婚恋网站物色单身女性，在网上下载其他男子照片，编造虚假身份，冒充“高富帅”实施诈骗。此外，该诈骗团伙为了提高作案成功率，特别聘请心理学博士起草诈骗话术脚本，进行话术培训，可以在聊天时更好应对欺骗受害人。

根据警方提供的数据，相关“杀猪盘”式特大跨境系列网络诈骗案涉及受害人 1500 余人，涉案金额高达 3000 余万元。受害女性年龄大多集中于 30 岁至 45 岁，少数不足 30 岁，其中最大单笔被骗 300 余万。有的受害人投入了全部积蓄，连带借遍亲戚朋友，还有从各种小贷公司“融资”，甚至卖车、卖房，直到最后醒悟时才追悔莫及。

案例二：利用新冠疫情进行诈骗

2020 年 1 月底，上海的鲁女士发微信朋友圈表示：打算献爱心采购一批防疫口罩，向有需要的人员进行捐赠。颜某看到消息后主动联系上了她。颜某自称是长居美国的富豪，系美国很大的生意家族成员，甚至经营有石油生意，从境外代购一批口罩回国并非难事，而本次大量的医用口罩货源，他可用私人飞机包机运输回国，运输费用也可全额免单。

鲁女士对“洋阔少”的信誓旦旦毫不怀疑，与对方约定以 166 万余元人民币的价格代购约 11 万只某品牌 N95 型号口罩，并陆续向颜某支付 16 万元及一部 Iphone11 Pro Max 手机作为定金。

两周后，颜某谎称该批口罩已到达北京的机场，要求鲁女士支付尾款 140 余万元。鲁女士要求拿到运输航班号，并见货后再支付尾款，但颜某无法提供相关信息，察觉异样的鲁女士于是向公安机关报案。

经公安司法机关查证，颜某实际的经济状况比较困难，也没有美国绿卡并已被纳入“失信人黑名单”。在收取被害人定金后，也并未购进口罩运输回国，而是大肆挥霍。最终，颜某因犯诈骗罪被判处有期徒刑 6 年零 6 个月，并处罚金 5

万元。

案例三：利用网络赌博进行诈骗

2020 年 2 月，安徽居民陈某在微信群里，下载了一个群主推荐的麻将游戏 APP，输了 100 元后，陈某卸载该 APP 并退出微信群。但几天后，该微信群主阮某就一直催其付款。陈某意识到这可能是新型诈骗，当即报警。

警方调查发现在当地，除了阮某外，还有李某、陈某两人也以类似手法招募人员参赌，并从中获利。据查该 APP，除了有当地的麻将玩法，还有江苏、四川、福建等地不同形式的玩法，每日参赌者近千人。5 月，警方专案组在当地将阮某、李某和陈某抓获。

三名嫌疑人交代：其通过微信群招募参赌者，再于 APP 内开设多个“房间”组织赌博。每局终了，统计胡牌进行加减分，然后根据得分以乘以 2 元、5 元和参赌者进行结算。但每局结束后，每位参赌者须缴纳 2 至 4 元不等的“房费”。同时，警方发现阮某、李某和陈某三人互不认识，只知道相互的微信号，但三人都会从一个叫黄某的手中购买 APP 的“房卡”，并称黄某是该 APP 在当地的总代理商。警方立即将黄某抓捕归案。黄某供述：其于去年 12 月看到网络赌博平台招募代理商，为图高利润、高回报，便与这个网络赌博平台的代理人龚某联系。龚某要求黄某将当地的麻将玩法告诉他，用于制作相关麻将赌博软件，并承诺让黄某作为当地代理商。不久，当地麻将 APP 正式上线，黄某也成为该 APP 的当地代理商。黄某和龚某达成交易：龚某负责赌博网络平台运维，黄某则负责发展本地参赌者。黄某自己不招募参赌人员，他主要招募下级代理商，将较低价格购入的“房卡”加价后出售给二级代理商，谋取利益。

经过大量调查，警方最后发现该赌博 APP 是由成都某科技有限公司研发，其幕后老板系张某。张某于 2016 年成立该科技有限公司，在 2018 年 8 月意外地收到来自安徽的一个订单，要求帮助客户搭建一个网络赌博平台。在其后短短三个

月内，张某帮助客户建成了一个赌博 APP，成功获利十几万元。为逃避法律打击，该公司将网络赌博 APP 下载服务器设在境外，并在同一办公楼成立短视频运维工作室作为掩护。在不到一年时间里，该公司共制作 20 余款赌博游戏，在全国多地招募代理商近 200 人，非法获利 50 余万元。

案例四：非法买卖个人信息

自“净网 2020”行动开展以来，珠海警方在网上巡查中发现有人公开销售珠海、澳门公民个人信息，便迅速开展网上线索跟踪和调查取证工作，于 2020 年 5 月在中山市抓获犯罪嫌疑人郑某，当场查获作案手机 2 部，其云盘存储非法获取的公民个人信息数据近 120G。

警方利用大数据分析研判发现，郑某与从事车牌查档业务的陈某长期非法置换公民个人信息，进而开展车牌、房产等信息查询获利的非法行为。随后，警方在中山市某政务服务中心附近将陈某抓获，现场查获作案用手机、电脑，其云盘储存非法获取的公民个人信息数据约 160G。次日，警方抓获陈某的上线姚某，查获作案手机 2 部，涉案云盘数据 62G。

经调查，犯罪嫌疑人郑某通过倒卖、交换公民个人信息，再置换、出售个人房产、车辆等相关公民信息，已违法获利近 30 万元。陈某借助在多地某房产公司的任职便利，非法获取公民个人信息，并向郑某、姚某出售，仅进行查车、查房违法行为就获利近 1 万元。姚某通过违法查询车牌信息出售车主公民个人信息近 3000 次，获利 3000 余元。目前，经检察院批准，上述三名犯罪嫌疑人已被依法逮捕。此外，警方通过对数据研判，对案件涉及的 4 家中介公司员工违法购买公民信息的行为进行了调查，并依法处以行政处罚。

案例五：非银行支付机构客户备付金挪用

2019 年 6 月，先锋支付的母公司中新控股发布公告披露：经过内部调查，其客户北京经讯时代科技有限公司（以下简称“经讯”），挪用先锋支付备付金账

户资金合计约 14.95 亿元。监管机构责令先锋支付填补该挪用资金，并且如果没有在合理时间内填补该资金，其支付业务将不被允许恢复运营，并且吊销支付业务拍照。

先锋支付成立于 2007 年，2013 年 7 月 6 日取得支付业务牌照，获准开展互联网支付及预付卡发行与受理（北京、辽宁）业务，并于 2018 年 7 月 6 日顺利续展。经过多年的发展，先锋系成为了庞大的金融帝国，但也引来不少质疑。先锋系网信理财上多为千万级项目，由先锋旗下的担保公司和保理公司担保，先锋支付划转，财富公司管理，海南农商行存管。围绕网信和中新，形成了整个集团的产业链。

调查发现，先锋集团成立了数百家壳公司，以这些公司作为借款主体并互担互保，向投资人融资，至少有 140 亿资金装入了先锋集团腰包。

先锋系旗下的多个分公司已被地方公安部门立案侦查。负责线下销售理财产品的北京盈华财富投资管理有限公司，在常州、西安、长春、沈阳、哈尔滨等多地的分公司被当地公安以涉嫌非法吸收公众存款罪立案侦查。

（四）未来风险演变趋势

一是伴随市场环境愈加复杂，各类风险相互伴生的特征将更加明显。随着金融科技加速发展，支付创新不断加快，各项业务渐趋融合，风险攻击将在今后一段时期内更全方位地渗透到信用卡申请、支付、营销、账户管理和资金流转各个环节，引发欺诈、信用、合规和操作风险交叠共振，潜在风险隐患不断扩大。

二是数字支付新业态背景下，移动端和境外欺诈风险将加速凸显。移动支付等创新业务迎来发展契机的同时，风险也随之加速从卡介质向移动支付渠道转移。此外，由于跨境支付市场参与主体日渐多元，风控能力参差不齐，跨境风险也将进一步蔓延，加之法制、监管、文化、产业环境等方面差异的影响，一旦发生跨境风险事件，监控处置和沟通协调难度将不断加大。

三是疫情影响资金需求更趋旺盛，套现套利行为或将扩大行业信用风险。疫情下市场资金短缺压力进一步升级，风险加快释放和传导，信用卡资产质量进一步承压，套现风险大幅上升。在此背景下，代还 APP 出现死灰复燃的迹象，需谨防新一轮违规代还引发的信用风险滋生蔓延。

四是犯罪手法进一步呈现专业化、团伙化特点，形成完整产业链。跨国化犯罪集团正在逐渐形成，借助大数据和人工智能等新兴技术，业务、规则、技术等环节中快速寻漏能力不断加强，并呈现团伙作案、深度隐匿、全网流窜等特点，欺诈风险防控难度将不断加大。

五是违规创新滋生风险隐患，行业合规风险防控压力不减。受市场竞争加剧和利益驱动影响，个别机构盲目、无序创新，风险管理环节薄弱，易被不法分子利用，将支付接口提供给境内外非法平台使用。加之聚合支付服务商通过违规包装、整合和拆分交易以掩盖真实场景，加大了合规风险防控难度。

六是支付信息安全形势更加复杂，潜在泄露主体和环节将不断增加。伴随支付链条延展，可接触和处理账户信息的参与主体和环节增多，但各参与主体的信息安全管理水平良莠不齐，部分系统存在技术短板，加之网络攻击和信息窃取手段快速翻新，使得网络信息安全形势愈发严峻。

七是新兴支付方式或引发新型风险，并呈现风险洼地效应。支付业务形态变革、商业模式创新和业务范围延展，人脸支付、无感支付等创新业务陆续上线。新兴业务监控体系可能存在不完备、联动机制不健全和信息上送不完整等问题，极易成为被欺诈分子攻破的风险短板。

三、数字支付时代风险防控对策

（一）风险防控总体架构

传统基于简单规则逻辑和经验判断的风险防控手段已不能应对快速变化的

风险形势，为迎接数字支付时代各类风险挑战，支付业务各参与方应搭建贯穿事前、事中、事后全流程全方位的智能风险防控体系，实现事前风险管理标准化，主动预防、深入管理；事中风险监测智能化，精准打击、实时反馈；事后风险处置规范化，快速反应、关联排查。

1.事前客户身份识别、信息安全管理及产品安全设计是风险防控的第一道防线

（1）客户身份识别

对于发卡银行、应用服务方等面向用户的机构，应有效识别客户身份，尤其在个人 II、III 类银行账户线上渠道开立，信用卡线上发卡及授信，应用服务方账户开通等非面对面场景下，目前主要核验银行卡号、手机号、姓名、证件号的一致性，建议通过增加人脸识别、身份证复印件比对、验证身份证有效期等方式加强客户身份核验，并结合大数据技术对客户风险画像进行评估，相应设置授信额度和用户标签。

对于收单机构，重点加强商户身份识别，制定商户准入政策，特别对于商户线上自助入网的情形，应采取有效手段防范虚假商户风险，确保商户信息真实有效，同时对商户进行分级分类管理，配置合理的商户限额。

（2）信息安全管理

业务参与方在用户信息采集、传输、存储、使用、销毁全生命周期环节，均应遵循相关法律法规、监管政策及行业规范，按“最小化”原则采集用户信息，并确保相关系统安全性和管理规范性，防范系统被外部机构攻击引发的信息泄露事件，以及内部人员导致的信息外泄。

此外，建议业务参与方利用新型支付技术，例如通过支付标记化技术，对银行卡主账号用支付标记（Token）进行替代，从根本上杜绝卡号信息泄露的可能性。同时，还可通过支付标记域控技术，对标记应用范围进行限定，进一步降低

支付标记信息泄露风险。

（3）产品安全设计

一是将风险防控手段前置到产品设计中，例如对于异常设备登录情形增强用户身份核验，针对新老用户和不同业务场景分别设置限额等；二是产品应采集上送风险监控要素，尤其是终端唯一性标识，终端网络及位置信息等，并可利用设备指纹等新兴技术，采集更为丰富的设备信息。

2.事中依托智能风控体系实现可疑交易侦测，形成风险防控的第二道防线

支付业务各参与方应以风控信息为基础，运用大数据、关联图谱、人工智能、云计算等技术，搭建包含专家规则、有监督与无监督机器学习建模平台，建设具备实时、准实时和批量监测模式和风险管控能力的智能风险监控系统，还可进一步形成交易风险评分、风险标签等输出给前端产品或其他业务参与方，以便相关业务主体据此采取交易阻断、结算资金暂缓、弹窗提示、限额管控、用户身份增强验证等辅助风控手段。

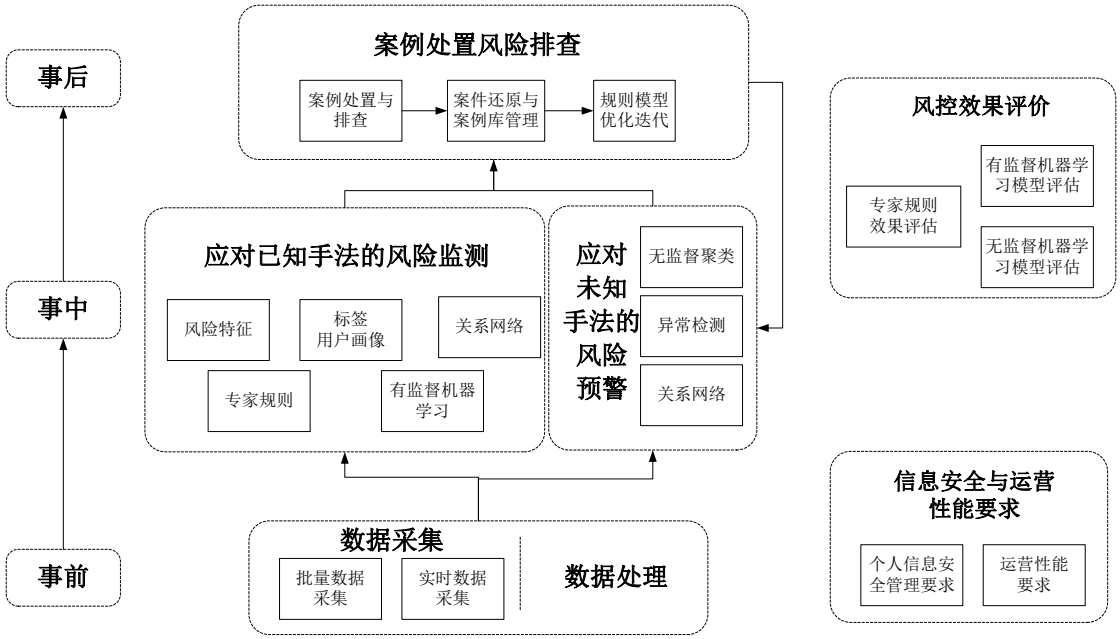
3.事后可疑交易协查及风险事件处置，损失挽回、贷后催收及风险信息共享构筑风险防控的第三道防线

首先，对于风险监控系统识别的可疑交易，应配置相应人力进行外呼调查或发送相关机构进行协查。对于确认的风险交易，需进行关联排查，挖掘关联卡片、设备、商户等维度的相关风险。针对规模性风险事件，产业各方应联合进行风险处置，防止风险蔓延；其次，借助行业联防联控平台，通过货物拦截和资金延迟结算各类手段，及时挽回已形成的风险损失，对于信用卡业务，贷后智能化催收也是信用风险管理的重要一环；最后，行业各参与方之间应共享风险信息，减少信息壁垒，防范作案团队在不同的机构、网络、业务之间使用相同作案手法轮番作案的风险。

（二）智能风控体系建设

智能风控体系作为风控中台，为业务应用提供实时高效的智能风控服务输出。业务应用既是风控系统的服务对象，又是风控系统业务数据的基础输入源，风控系统需要采集业务应用系统的相关业务数据，用于后续风险特征、风险标签、人卡机关联信息等风控数据的加工。

智能风控体系建设包括事前风控数据采集与处理、事中风险监测与预警、事后风险排查处置三个部分，整个体系基于风控指标开展效果评估，并基于效果评估不断优化完善，同时应符合信息安全要求并满足运营性能需求，总体应用框架如图所示。



智能风控总体应用框架图

1. 事前风控数据采集与处理

风控数据采集及处理是风险监测的前提，通过收集处理各类信息数据、行为数据、位置数据，全面描述交易主体的行为动作、关系、目的等属性；在数据采集过程中，需要清洗整理形成结构化数据，并抽取其中的重要信息，最终输出各种维度的数据、报表、图像、语音等形式的信息，从而为后续风险交易的风险特征提取打下基础。

对于业务应用的数据采集，主要有批量数据采集与实时数据采集两类，批量数据采集通过数据仓库等技术将业务应用的相关数据批量采集到数据库进行存储，再利用数据库计算能力对采集的数据进行逻辑加工，形成风控所需的风险特征、风险标签、人卡机关联信息等风控数据，并保存在智能风控体系的风险数据库内，为后续多维决策体系、智能预警、智能运营风控应用服务提供数据支撑；实时采集则通过安装在业务应用 APP 中的 SDK 或 API 实时将风险数据推送给风控系统。同时，智能风控体系可通过外部数据接口服务，同步外部风控数据存入风险数据库内，作为采集应用业务数据的有效补充，共同用于风控数据加工与风控赋能输出。

2.事中风险监测与预警

风险监测与预警是指基于风险数据，对交易行为动作执行过程的疑似风险交易进行实时或非实时性的干预，根据作案手法是否已知，可以分类为对已知手法的风险监测和对未知手法的风险预警。

对于已知手法的风险监测主要基于风险特征、标签画像和关系网络，通过“专家规则+有监督机器学习模型”的方式识别风险交易：**风险特征**是对风险行为的刻画，可直接用于与监测对象比较；**标签**是对某一类特定群体或对象的某项特征抽象分类和概括的结果，标签值具备可分类性，**用户画像**由某一特定群体或对象的多项特征构成，可理解为多个标签的集合；**关系网络**是利用图的数据结构来表达现实问题中复杂的业务关系，并通过大规模的图计算算法，发现关联性风险，识别不法团伙；**专家规则**是指该行业内具有丰富实践经验的风控专家，将已识别风险行为中具有某些特定特征（或特征组合）总结成具有因果关系的运行法则；**有监督机器学习**根据已有的标签，通过提取风险行为的有用特征，构造特征到标签的映射，建立模型，实时识别用户风险行为。

对于未知手法的风险预警主要采用无监督机器学习模型、聚类分析以及关系

网络等方法，开展异常检测，从而预警新型风险行为：**无监督聚类**是常见的数据挖掘手段，适用于小额高频特征的交易监控。其主要假设是风险行为往往表现为大规模团伙形式，也就是“坏人扎堆，好人分散”，故可以通过无监督聚类的方式抓取异常团伙，例如虚假账户注册等场景；**异常检测**是在无监督模型学习中比较有代表性的方法，即在数据中找出具有异常性质的点或团体，常用于检测抓取大额低频交易特征；**关系网络**也可以应用于未知手法的预警，当异常关系聚集出现时，即可识别风险行为。

3.事后风险排查与处置

风险排查处置是智能风控应用的重要环节，目标是排查潜在风险，控制损失敞口，迭代优化风控规则模型。

案例处置与排查时需要机构配置相应人力资源，对于触发风控系统的可疑案例开展调查、核实、反查以及账户止付、损失挽回等处置工作，并对于确认涉及风险交易的收款卡、付款卡、智能设备、商户进行关联排查，挖掘出更多的风险交易。

案例还原与案例库管理是对于确认为风险交易的案例开展分析、研究、总结和管理，是规则模型优化迭代的一项重要参考来源。案例还原是对案例分析研究的过程，其目的是研判案例中是否存在作案手法上的变化，以更新完善现有侦测系统中规则或模型的侦测效果。风险案例库管理是对于日常工作中发现的风险案例，根据案例的表现特征、是否未知风险、发生渠道以及来源等维度分类汇总。风险案例库内容可包含对欺诈场景的还原、作案手法和过程总结、揭示风险点等内容，特别是对典型和新型案例的分析研究。风险案例库的建立是为机构内部查找、补充、完善案例相关情况提供基础，同时也为同业案例分享提供可能。

规则模型优化迭代的来源分为调查确认案例总结和未知案例特征分析。前者是以案例调查中确认的特征为基础，跟踪已知案例作案手法变化，形成新的规则；

后者是使用不依赖于数据标签的无监督机器学习技术，侦测未知作案手法模式，发现未知案例异常特征后形成新规则，丰富规则引擎，扩展规则侦测的识别能力。两者都是对规则引擎的补充和完善。

4.智能风控效果评估

可运用风险指标评估其智能风控规则和模型的应用效果，基本风控效果评价指标包括欺诈率、覆盖率、打扰率、准确率、误报率等；有监督机器学习模型和无监督机器学习模型应用效果评价指标还包括 PR 曲线、ROC 曲线/AUC、F1 分数、轮廓系数等。

欺诈率指风控系统未侦测防控的欺诈交易金额占所有（经风控系统）交易总金额的比例。它的变动能够量化通过智能风控体系控制风险的能力。

覆盖率指所有交易中，风控系统侦测出的所有疑似风险交易占所有（经风控系统监测）交易的比例。

打扰率所有发生交易的客户中，风控系统侦测出的所有疑似风险用户占所有（经风控系统）交易用户的比例。打扰率直观的反映了所有用户中，多少用户会被打扰。正常用户经常性被打扰会降低用户体验。

准确率指风控系统侦测出的风险交易占所有疑似风险交易的比例。

误报率指风控系统侦测出但确认非风险交易的正常交易占所有疑似风险交易的比例。

PR 值是相互矛盾的指标，分别代指准确率(Precision)和覆盖率(Recall)。一般情况下，准确率越高则覆盖率相对会低，同样覆盖率提高，准确率相对会降低。

5.信息安全与运营性能要求

机构开展风险防控时，需遵循相关安全要求，在合法依规前提下采集、保存、处理及使用个人信息。首先，收集个人信息前，应向个人信息主体明确告知收集

的个人信息类型、使用、委托处理与共享的规则和目的、存储期限等，并获得个人信息主体的授权同意；其次，传输和存储个人敏感信息时，应采用加密等安全措施，在保存时需要限定保存时间长度，并进行标记化处理；最后，个人信息在展示和使用时，需要进行必要的脱敏，并控制使用期限和使用范围，对于超出使用期限的个人信息，必须及时销毁，以免造成数据泄露。

智能风控体系交易监测与数据处理方式需要匹配业务风险防控需求，确保风控运营流程顺畅。对于实时监控与拦截，在风险交易会立即造成损失的情况下，需要实时返回处理结果，且交易处理能力要与机构业务风险防控需求相匹配，对资源配置、特征计算方法、模型准确性的要求较高。对于准实时监控，在延迟决策或决策时效性要求不太高的情况下，响应时效要求可略微放低至秒级或分钟级，对资源配置要求也相应降低。对于批量监控，定期触发，对资源的配置要求不高，适用于在较长周期内进行回溯排查。

（三）应用实例及经验分享

案例一：工商银行牡丹卡中心构建智慧风控新生态的应用实践

工商银行信用卡风控体系经历了以人工方式进行经验控制的“人控”时代和以风险管理系统为基础的“机控”时代。近年来，工商银行深入探索行业领先风控技术和金融科学前沿知识，积极构建智慧风控新生态，一方面充分利用系统、数据、模型和策略，建立大数据风控体系，一方面积极发挥传统线下优势，通过专家经验和组织架构解决差异化需求，构建新型智慧风控生态系统，为客户日益多样化的金融需求保驾护航。

在欺诈风险防控方面，工商银行通过引入生物特征识别技术，通过模型及算法对用户操作行为、操作习惯进行分析，从而识别异常行为及高风险客户，降低欺诈风险；例如，采用传感器用户认证技术，通过分析用户操作手机行为习惯识别欺诈（非本人操作）行为。在信用风险、合规风险防控方面，工商银行应用关联图谱技术甄别信用卡及个人信用贷款违规风险，通过构建资金在不同客户、商户实体的流向知识图谱，及时识别资金违规用途，大幅提升资金流向违规领域等监控的精准度及时效性。

工商银行将进一步倡导“数据文化”理念，推进“机智”与“人智”有效结合，坚持总分行双轮驱动，全面提升风险管控的精细化和智能化水平，形成了业务发展与风险管理协调并进的良好局面。

案例二：平安银行贷款业务智能风控技术应用

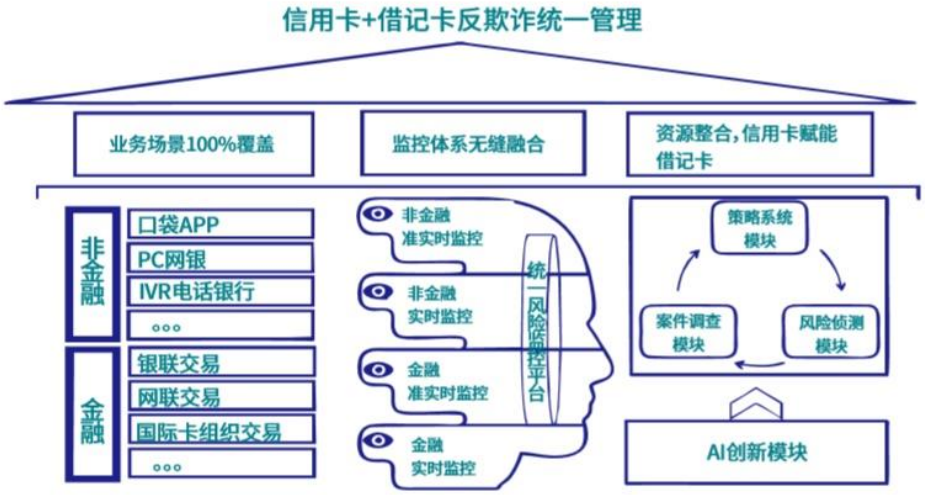
平安银行在信用卡业务中有效运营智能技术，实现了在贷前、贷中、贷后三个流程的应用，已建立一整套涵盖审批、授权、催收各环节的智能风控体系，在不断提高风控能力的同时，给予用户申卡、用卡的最佳体验与保障。

一、贷前——智能审批，打造极致审批体验

通过智能预审平台让用户在申卡前简单快速的获取预审额度，在审批时，基于不断迭代优化的算法+模型，加以人脸识别、活体检测、微表情分析等 AI 技术的应用，采用智能审批机器人实现系统审批，在风险有效控制的前提下，让用户能最快得到审批结果。

二、贷中——智能交易授权

平安银行建设了场景式实时交易授权决策系统，能从账户级的决策进入到交易级的决策，通过后台的评分系统和决策体系，对伪冒、套现等风险都能做到对当笔交易的实时管理。此外，平安银行对信用卡、借记卡的伪冒和授信进行统一管理，把防伪冒全套系统整合在同一个团队，使银行零售方面特别是借记卡交易的伪冒管控能力得到了大幅提升。



三、贷后——智能催收管理

平安银行在贷后催收管理方面也采用了目前行业中较为创新的做法，即让机器人像优秀的坐席一样为客户提供实时在线语音账务服务，运用风险标签罗盘，进行差异化催收。

面对日趋复杂的风险形势，平安银行全力研究把握前沿技术，构建智能风控的应用实践框架，全面提升银行风险管理能力。

案例三：银联商务收单业务创新风控架构构建经验分享

银联商务通过总结十余年的风控系统建设经验，基于将特约商户、用户、支付账户及增值服务四类等行为主体进行统一观测的理念，形成了以全新风控系统WATCH 3.0Watch2.0 为核心的风控架构设计，通过平台数据整合及高效智能的识别算法等，借此发现客户所有的关联风险行为，并实现多主体间的身份联动监控，并配置智能化、电子化的决策干预及调查处置流程，以满足风控快速对接、快速部署、快速运算的“三快”业务需求，为内外风控赋能及产业合作提供强有力的支持。

银联商务 WATCH2.0 风控技术架构图

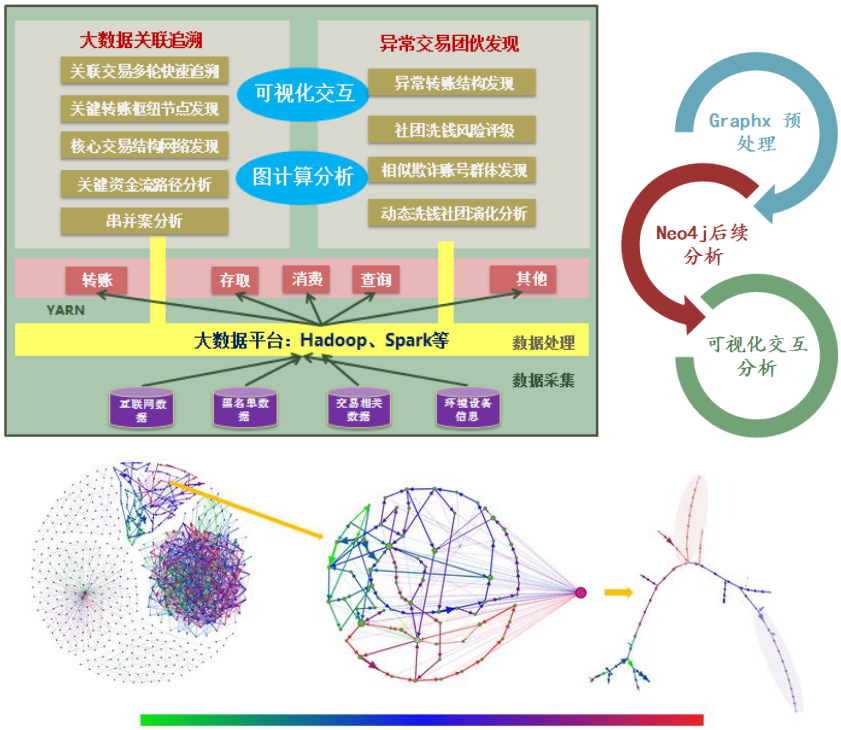
在关联图谱侦测实践中，银联商务取得了良好应用效果，通过对商户的基础信息和交易构建动静态信息结合的图谱，结合异常监测结果和业务指标圈定可疑社团，能有效识别打击营销欺诈灰色产业链以实施团伙欺诈为目的的特约商户入网申请，提升风险防范能力营销效果；对信用卡交易构建图谱，结合历史风险状况对可疑社团重点核查，能有效辨识套现灰色产业链中常见的套现交易分拆手法。在科技风控的浪潮下，银联商务投入了大量的资源提升自身的技术水平，并积极与产业各方合作推进创新技术在风控中应用，提升风控能力。展望未来，银联商

务将积极发挥自身能力优势，探索新型智能风控技术方案快速应用，推动支付产业的健康发展。

案例四：中国银联大数据反洗钱技术新探索

随着电子支付的兴起，更加便捷的支付方式也给犯罪分子提供了更多洗钱的渠道，以往的反洗钱规则系统越来越难以应对日益复杂化洗钱手法。为此，中国银联基于银联海量交易数据，深入探索支付领域反洗钱新技术方法，构建了一套基于智能风控分析技术的反洗钱解决体系框架。

该体系框架一方面可以有效利用已有反洗钱涉案信息进行全方位的关联追溯，充分发挥案例数据价值。另一方面能够主动地从海量交易数据中寻找高风险洗钱社团，发掘新的团伙化、集团化的洗钱交易模式，提升金融反洗钱工作效率，为国家金融风险防范、打击非法交易犯罪提供有力技术支撑。



在此基础上，中国银联创新研发了混合事件关联追溯、时序有向社团发现算

法以及洗钱社团风险评级等多种算法，实现了反洗钱行为的主动发现，推动了场景侦测从事后向事前的转变。

在业务场景纷繁复杂，风险形势日益严峻的支付业务发展态势下，中国银联将不断地完善反洗钱侦测技术研究和应用，结合频繁集项、分类聚类、深度学习等人工智能算法，进一步定位高可疑的洗钱交易模式，有效地进行链接挖掘和团伙侦测，协助相关业务参与方共同提升洗钱风险侦测分析能力。

（四）风控挑战

在与黑灰产业及作案团队的攻防战中，现有风险防控与侦测机制取得了阶段性成效，有效遏制了规模性、集聚性风险事件，但也面临诸多问题和挑战。

首先是监管要求提升，数据是产业风控发展的基础能源，但近年来随着大众隐私保护意识的觉醒、国家对个人信息安全管理的要求逐步加强，对数据采集、存储、使用等都提出了更为严格的规范，这也意味着原本对风控有关键作用的核心数据获取难度加大，且面临更大的法律和合规压力。因此，如何通过最小化的数据资产产生最大化的风控效能，进而平衡好信息共享、隐私保护和风控合规之间的关系，是摆在产业各方面前需要迫切解决的命题。

其次是参与主体增多，在数字支付新业态下，支付参与主体增加，一是参与方良莠不齐，易形成“短板效应”，任意一方的不作为或者存在薄弱环节都可能给整个产业带来风险，风险呈现传染性、交叉性的发展特点，防控压力与日俱增；二是参与方复杂，业务场景多变，信息呈现不对称、不透明的特点，例如发卡机构无法掌握实际业务场景和收单侧的完整风险信息，部分机构甚至为逃避其他参与方的风控机制，故意变造交易和风险信息。

最后是作案手法升级，在数字支付时代下，作案分子已呈现团伙化、专业化、智能化等特点，并在不断试探风险交易侦测逻辑，转变作案手法，如何应对快速变换的攻击手法是风险攻防战所面临的问题之一；另外，作案分子往往还利用分

身设备、伪造网络或地理位置等信息，使得风险侦测基于的风险信息失真，或利用短信嗅探等技术截取用户的身份验证信息，作案技术手法升级也是风险防控的一大挑战。

四、安全生态建设

（一）行业联防联控

产业风险联防联控平台建设对于安全支付生态建设有着重大意义，银行卡组织、商业银行、公安司法机关、非银行支付机构等产业各方通过联防联控平台强化风险交流联动和快速处置风险事件，共同促进银行卡产业的安全健康发展。

在产业各方携手推进下，业内已形成银联风险管理委员会、银行卡安全合作委员会、互联网金融支付产业安全联盟、多个同业交流平台、打击预防金融支付犯罪联合实验室等多层次的风控合作体系，并定期组织同业专家交流探讨行业新动态。其中，**银联风险管理委员会**致力于推动落实监管政策，强化司法合作，构建风险制度体系，开展风险联防联控，妥善处置各类风险事件；**银行卡安全合作委员会**负责搭建警银联动协作平台，推动公安司法机关与支付业务各参与方在案件侦破、司法协查等多个领域开展深入合作；**互联网金融支付产业安全联盟**推进产业全链条各机构间的新兴技术研究应用、风险信息共享、安全支付宣传等合作；包含信用卡风险防控高层研讨会、信用卡同业风险联席会议的**多个同业交流平台**，着力促进产业各方之间，以及与监管部门及立法机关之间，关于风险热点问题及前瞻性课题的沟通交流，分享同业风险数据与典型案例，研判风险形势和应对举措；**打击预防金融支付犯罪联合实验室**聚焦于针对支付犯罪新手法新技术进行攻防分析研究，推动强化支付防护手段。

多层次的风险联防联控平台机制对落实监管政策、推动法律环境和风险制度建设、加强风险信息共享、风险案件联动处置及共同打击银行卡犯罪、提升风控技术水平等发挥了重要作用，通过联防联控平台，产业各方正共同不断构建完善

数字支付安全生态圈。

（二）风险信息共享

面对愈加复杂严峻的信用、欺诈、合规等风险形势，交织伴生的共债、逾期、套现、非法交易、电信诈骗、信息泄露等问题，需要进一步加强行业风险信息共享，形成行业风险防控合力

多年以来，商业银行、非银行支付机构与银行卡组织之间已建立形成银行卡风险信息共享机制，共享内容涵盖黑灰名单风险数据、风险指标、风险案例等多个方面，该机制已得到行业各参与方的广泛认同，成为发卡开户风险审核和收单商户入网审核的必备流程。针对新风险形势下机制、业务和技术等层面的新诉求，产业各方在原先共享机制的基础上，进行整合、优化、补充和完善，从风险“黑/灰”名单数据共享、风险事件案例分享处置、风险能力合作研发、风控策略共建、趋势研判五个层面丰富新信息共享机制的内容和内涵，进一步提升信息共享所带来的价值赋能。

在银行卡风险信息共享机制的基础上，公安机关、商业银行、支付机构、银行卡组织，以及大型电商、安全厂商、终端制造商等产业上下游单位，依托互联网金融支付产业安全联盟等行业合作平台，开展风险信息共享合作，进一步扩展信息共享参与主体。初期联盟通过信息集中报送后再分发的方式，实现了行业普适性风险信息的共享。2018 年起，联盟试点运用区块链技术创新建设风险信息分布式查询机制，通过区块链技术加强共享数据的安全保密性，同时明确机构间进行共享的业务风险场景，协助数据所有方实现数据资产价值，提升共享与应用的时效性，引入共享评价机制，提高机构参与意愿。通过产业各方共同努力，“多元化、多层次、多维度”的风险信息共享机制不断推进，机构间的风险案例互动分享和风险事件联动处置更为紧密，对产业风险防控及安全生态建设发挥了积极作用。

（三）持卡人支付安全意识培育

近年来，数字支付产品已经基本覆盖日常生活的主要场景，支付风险形势也愈发复杂，迫切需要持卡人提升自身安全意识，从根源上降低风险发生的可能。根据权威机构移动支付安全调研显示，国内用户在使用移动支付时，依然存在诸多不良使用习惯，如更换新手机时，不解绑银行卡或删除存留的敏感信息（24%）；直接删除带支付功能 APP，不解除银行卡绑定（23%）；带有优惠信息的二维码都尝试扫描（20%）等，针对数字支付时代新型支付安全知识的普及工作，依然任重而道远。

长期以来，人民银行等监管机构在安全宣传、风险防范等方面坚持“支付为民”的理念，产业各方在监管机构的指导下，积极探索完善多层次的支付安全宣传机制，共同向广大持卡人持续普及金融支付安全知识，提升用户支付安全意识，并取得了显著成效：**一是**每年定期开展 3.15 金融消费知识普及宣传、5.15 打击和防范经济犯罪宣传，组织开展金融联合宣传教育、支付安全宣传月等专项活动；**二是**通过微信、微博、官网等渠道，推送风险防范知识软文及风险提示信息，发布语言通俗、图文并茂的宣传稿件；**三是**定期开展移动支付安全大调查等活动，并通过主流媒体向全社会发布调研成果。**四是**开展了多种多样的线下活动，推进金融知识进社区、进校园、进网点、进企业。

（四）消费者权益保护

随着金融科技的快速发展，我国支付市场正在发生复杂深刻的变化，供给侧开放进入全新阶段，需求侧变化迎来日新月异，监管机构工作机制和规章制度不断完善，消费者权益保护成为数字支付时代下产业各方面临的重大课题。

在监管机构的指导下，产业各方秉承“以客户为中心”的原则，扎根服务实体经济，促进普惠金融发展，不断健全完善金融消费者权益保护工作体系：**一是满足消费者多元化支付服务需求**，持续推进支付产品和服务不断优化创新；**二是加强消费者个人隐私数据保护**，从数据收集、存储、加密、传输、使用、共享、删除等全流程环节做出详细规定，为消费者个人隐私穿上严密的防护服；**三是畅**

通客诉处理渠道，积极保障消费者投诉“进得来”，随时得到受理，又能“放得下”，获得有效的后续处理，切实保障客户满意度和投诉处理效率。**四是加强产品与服务全流程风险防控**，构建一体化智能风控体系，充分利用生物识别、大数据、人工智能等技术手段，保障消费者资金财产安全；**五是大力开展金融知识安全普及**，从源头推进消费者权益保护。

数字支付时代下，随着消费者的需求更为个性化、场景化，消费者面临的威胁与挑战更为复杂，对自身权益保护的意识也逐步提高。产业机构需要进一步完善消费者权益保护体系，加强联防协作，共同推动解决突出问题，合力推进支付产业规范创新发展，提升消费者权益保护水平。

五、结论和展望

（一）基本结论

面对数字支付时代业务市场发展和风险形势，在监管政策指导和业界各方风险防控应对之下，支付产业安全生态初步形成，业务安全逐步加固，行业风险总体可控。

1.监管政策落实更加坚决和到位，行业“正本清源”取得阶段性成效

根据监管要求，整个支付产业加强了对无证经营屡禁不止、创新过程金融风险多出、共性问题屡查屡犯、垫资结算风险初露苗头等监管高度关注问题的整治，并持续开展伪冒开户、备付金挪用等重点业务的风险侦测，对于电信诈骗和网络赌博等突出风险进行打击治理，确保监管要求落到实处，行业“正本清源”取得阶段性成果。

2.产业风险防控认识不断加深，新兴业务和新型支付风险引起各方重视

随着支付产业进入新的发展周期，业务创新不断涌现，作案手法技术更新迭代，各类风险事件层出不穷，风险交织并存的特征越发明显，产业各方对于风险

防控的认识也不断加深。代还 APP、新型电信网络诈骗、网络赌博、系统攻击等新型支付风险已引起各方关注和警惕，配套部署了相应风控手段。

3.各类新型防控技术及手段快速应用，风险敞口得到一定控制

为应对日益严峻的风险形势，多数机构积极运用新型防控技术，建设智能风控体系，推进智能风控应用。针对新兴业务风险特点设计智能风控模型，并基于用户标签及画像、机器学习、关系网络挖掘风险特征，侦测识别可疑交易，风险敞口得到一定控制。

4.产业风控合作愈发主动和高效，支付安全生态初步形成

在产业各方的推进下，风险防控合作更加主动高效，已搭建公安司法机关、银行、非银行支付机构、安全厂商等多方位多层次的合作平台，并在争取法律政策支持、增强产业风控合作、打击银行卡犯罪等工作中取得了成效；针对 C 端用户，已建立常态化支付安全宣传机制，切实保障消费者权益。

（二）未来展望

虽然风险防控取得一定成效，但在宏观经济下行、严监管常态化的形势下，整个产业开始进入整固调整的新发展周期，各类风险隐患依然存在。展望未来，风险防控任重道远，产业各方应凝心聚力，共同推进以下工作。

1.准确把握严监管常态化的政策形势，以“支付为民、风险为本”为初心，持续落实监管政策要求

尽管风险形势严峻复杂，监管要求日趋严格，风险防控压力和挑战空前，但也为整体支付行业持续强化风险管理能力提供了宝贵契机，支付业务各参与方更应提高政治站位，把握风险防控的重点和节奏，以“支付为民、风险为本”为初心，持续落实监管要求，净化产业环境，为行业发展提供正向的支持和保障。

2.紧密跟进产业业务及风险动向，高度警惕新型业务风险，妥善处理风险防范与业务创新之间的关系

创新是支付产业发展的内驱力，而安全是支付产业发展的基础，产业各方应坚持并倡导负责任的创新，摈弃过度和无序创新，积极化解创新过程中存量风险。同时，紧密跟进产业业务及风险动向，高度警惕新型业务风险，妥善处理风险防范与业务创新之间的关系，共同寻找创新发展和风险防范的最佳平衡点，为业务健康可持续发展保驾护航。

3.积极运用大数据、智能风控技术，推进行业风险防控能力全面升级，提升新业态下的风险防控能力

业务参与各方应加快建设智能风控体系，积极借助技术手段建立起全流程风控闭环，实现从重事后处置向事前主动预警、事中监控和事后处置整治结合并重的风控新模式转型。重点针对线上新型网络犯罪，以机器学习、生物识别、云计算等技术为抓手，构建全天候全方位的风险态势感知体系，提升精细化的风险侦测预警能力，对犯罪团伙实现精准打击。

4.着力推动安全生态建设，完善新业态下多层次风险合作平台建设，提升公众支付安全意识以及消费者权益保护

首先，产业各方需进一步推进建设多层次、常态化、有深度的联防联控合作交流平台，深化平台成员交流机制，进一步提升行业联防联控水平；其次，强化行业内风险数据共建和共享，在合法合规的基础上，扩大参与机构数量，提高数据质量，消除数据信息碎片化，形成合规、高效、开放的共享新局面；最后，持续开展持卡人支付安全教育，营造安全用卡环境，提高对消费者权益的保护，共同创建产业安全新生态。

（三）呼吁及建议

为进一步提升产业风险防控水平，开创产业风险防控新局面，共筑安全和谐的支付生态新环境，对相关业务参与方提出以下建议：

1.法规监管层面

（1）完善相关行政监管及司法治理模式，多头并举合理化解套现风险

目前，套现风险特征已发生明显变化，对于职业化、团伙化及通过网络向不特定主体提供套现服务的犯罪活动，特别是职业犯罪和为赌博、电诈等非法活动提供套现服务等社会影响恶劣的犯罪行为，建议按照“区别对待、精准施策、疏堵结合、联防联控”的原则，行业行政监管与刑事打击并举，把握好刑事介入打击犯罪的门槛，并为持续发展变化的经济活动留有一定空间，如对小微企业以“融资救济”为目的的信用卡套现行为采取一定的容忍度。

（2）强化监督检查和打击处罚，提高参与方违规成本，健全线上收单业务约束

目前少数收单机构信用卡收单业务发展策略较为激进，甚至对交易进行变造，透传给发卡银行的信息严重失真，套现客户、商户信息难以查实举证。建议监管机构进一步加强对收单机构业务的监督检查，从严规范收单业务合规管理和风险管理，对违规收单加大惩处力度，提高违规成本，同时，建立健全收单线上支付业务的监管约束机制，加大对代还 APP 等新型套现的打击力度。

（3）完善征信体系，防范过度授信，降低共债风险

客户负债情况是贷前审核的重要依据，但当前征信体系尚在逐步完善过程中，客户的网贷、小贷等非银行征信数据难以全面获取。建议监管能够打通互联网金融借贷数据和银行数据，以便发卡银行能够更加精准地识别客户风险和负债水平，防范过度授信，减小共债风险的传播，保障行业整体信用风险可控。

（4）建议加大对代办、代养、反催收等黑产的法律惩治力度

信用卡黑灰产已从传统线下作业向智能化、体系化的线上模式转变，且已逐步演变成贯穿包装办卡、代还养卡及反催收投诉为一体的产业链条，大大增加贷前审批、贷中处置和贷后催收的复杂性。其中，影响最大的是“反催收联盟”等灰色组织教唆、拉拢并煽动逾期借款人恶意利用监管要求阻碍银行正常催收工作

的行为，对贷后清收效率产生严重阻碍。当前刑法对代办信用卡、反催收联盟、线上代还养卡等暂无明确的认定和打击标准，即使查处也无法入罪入刑，对不法分子的震慑力度不足。建议明确对套现办卡黑中介、套现商户、代还平台和恶意反催收等行为的违法认定标准，加大打击与惩戒力度，将打击非法中介纳入刑事打击范畴。

2.行业规范层面

（1）加强监管政策解读，协助行业各方准确把握文件要求

严监管形势下监管文件频发，各家机构对监管发文等政策制度理解存在角度不同、执行标准不一的情况，建议围绕法律法规和监管政策，面向机构加强专题解读培训，帮助产业机构准确把握政策内容和要求，确保相关工作落到实处。

（2）优化数据传输交互方式，推进风险信息透明化

部分创新业务中，交易付款方 IP、账户 ID 等应用服务方账户侧关键风控要素信息，其他业务参与机构无法获取，可采取的风控措施较为有限；部分业务模式下，个别业务参与方缺少实时交易流水，难以自主采取实时和准实时等时效性较高的风险监控措施。建议建立优化数据传输交互方式及业务参与方间的数据信息通路，推进风险信息透明化，为参与机构风险决策提供数据支持。

（3）进一步提升信息安全管理要求，对违规行为进行集中整治

由于少数收单机构信息安全管理机制仍有待完善，个别代还类无证支付 APP 在信息采集、传输、存储及使用等环节仍存在安全隐患，同时随着代还 APP 整治工作的推进，此类 APP 的业务开展受阻，极有可能引发前期留存信息被贩卖的风险隐忧。建议监管机构和行业平台进一步提升信息安全管理要求，联合产业各方深入推进对违规留存账户信息行为的集中整治，并第一时间将相关事件进行全行业通报。

3.产业合作层面

（1）扩展行业风险信息共享范围，深化风险合作机制

当前欺诈手段变化多样，专业化、职业化程度高，相关作案手法经互联网传播、复制的速度非常快，建议相关产业协作平台在风险信息共享的基础上，增加风险案例的共享机制，便于机构及时了解掌握最新的犯罪手法和技术的变化趋势，及时布署风控策略。

（2）建立系统化风险案例推送协查机制，增强风险处置效率

部分机构现有日常风险案例推送协查尚未完全系统化，存在因手工处置时效性不高，导致风险资金已转移、未成功挽损等情况。建议加快推进风险线上处置对接平台建设，提升风险事件一体化处置效率，同时研究对部分风险商户进行先行处置的可行性。

（3）切实加大支付安全知识的普及力度，提升持卡人风险防范意识。

数字支付时代，支付产业发展之根本在于支付安全。因此，提升持卡人安全支付意识日益迫切，建议将移动支付安全知识的普及落到实处，多渠道宣传移动支付风险案例和防范建议，培养用户良好的安全支付习惯，提升用户安全支付认知水平，切实让安全支付的理念深入人心。