数字金融反欺诈技术应用分析报告（2021年）

中国工商银行金融科技研究院安全攻防实验室

中国信息通信研究院云计算与大数据研究所

版权声明

前 言

我国数字经济发展迅速，特别是新冠肺炎疫情发生以来，疫情影响下金融行业全面加快了数字化转型步伐，当前数字技术已广泛渗透到智能支付、智慧网点、数字化融资等各个领域，金融机构朝着智慧化、开放化、生态化方向发展。在数字化转型大潮下，金融业务模式更加灵活、开放，在为客户提供更加优质服务体验的同时，也客观上给网络黑产滋生提供了更加有利的条件。

近年来，数字金融欺诈技术造成的损失和影响不断扩大，不仅作案手段不断翻新，甚至出现成熟的黑色产业链条，欺诈行为也呈现线上线下融合、跨机构作案等新型特征，给金融机构风险防控、公安机关追查打击带来更大的难度。

中国工商银行是国内金融科技的引领者，在严守生产系统安全、保障数字化转型的工作中，积累了大量与黑产斗争的经验；中国信息通信研究院是国内信息通信领域的主要支撑单位，参与了国家各项数字金融欺诈治理工作。此次白皮书编制结合了中国工商银行以及中国信息通信研究院的研究成果，对数字金融欺诈的形势、特征进行了剖析，并给出了金融行业在数字金融反欺诈方面的技术和应用场景。希望为关注数字金融反欺诈的企业、政府机构以及相关单位提供参考和帮助。

目录

一、数字金融反欺诈概述

（一）数字金融反欺诈发展情况

1. 金融业数字化转型浪潮下反欺诈形势不容乐观

在新一轮科技革命和产业变革的背景下，金融业数字化浪潮蓬勃兴起，大数据、人工智能、云计算等新技术与金融业务深度融合，成为推动金融转型升级的新引擎、服务实体经济的新途径、防范化解金融风险的新利器，数字化转型已成为金融业提高服务质量和竞争力的共同选择。

随着金融机构运用新科技进行创新转型的加速，网上银行、手机银行、移动支付等线上数字金融业务在带来更大创新空间，为客户带来更加高效、优质的金融服务的同时，也给反欺诈带来了严峻挑战。在巨大经济利益的驱动下，不法分子利用钓鱼链接、木马、电信诈骗等各种手段盗取、骗取客户资金的案件层出不穷。针对线上转账、支付等环节的欺诈，已经发展成为组织严密、分工明确的黑色产业链条，给客户和金融机构造成了严重损失。

2. 新型信息技术正在加速提升数字金融反欺诈效能

数字金融快速发展也催生了新的数字金融欺诈行为，数字金融欺诈本质上也属于金融欺诈，相较于线下金融欺诈和互联网金融平台陷阱，数字金融欺诈使用多重攻击手段联合作案，具有黑色产业链成熟化、欺诈组织职业化、作案目标精细化、欺诈活动移动化、欺诈事件高频化、欺诈行为场景化等特征，对数字金融行业的普惠目标和创新发展带来负面影响，给金融机构和金融科技企业的风控带来严峻挑战。

数字金融反欺诈是指利用数字技术进行金融反欺诈，即利用数字技术识别与预防数字金融欺诈行为，通过使用大数据、云计算、人工智能等新技术，可以建立新型的智能反欺诈风控系统，改变传统反欺诈的被动防御局面，帮助企业化被动为主动，提前拦截欺诈发生，具备高并发、低时延、高精度、高可靠等特点，可进行毫秒级的风险判定，并能够支撑实时的机器学习模型和智能风险决策。

（二）数字金融反欺诈即将进入全周期防控新阶段

传统的反欺诈系统主要基于被动防御模式，利用规则、特征等对每一笔交易进行事中识别，规则、特征都是基于已有的经验进行设定，很难识别一些新的攻击手段或是漏洞。数字金融反欺诈可以从事前、事中、事后三个阶段进行风险预警或识别。

1. 事前预防——客户画像

金融机构利用技术手段从金融服务客户端和网络公开信息中查找、搜集、整合数据，多维度多渠道的金融数据是使用金融科技反欺诈工具的基础。通过海量丰富的数据信息流，可以形成更为全面的用户画像，以便对潜在风险用户的欺诈行为进行预测和防范。在获得用户画像之后，更可以结合不同用户的数据内容，例如共用 IP 地址、通讯记录、交易记录等，构建包含海量用户的大数据关系图谱，有效防范团伙欺诈行为。

2. 事中应对——欺诈拦截

因应不同欺诈场景，数字金融反欺诈可以采取更具针对性的干预措施。第一类措施是通过金融科技反欺诈系统精准识别风险用户，防范并拦截金融欺诈行为，辅助互联网金融平台过滤可疑信息量。第二类措施是对金融平台上的交易行为进行风险估测，拦截可疑交易并通过验证码或人工方式进行核实，且在后台登记交易拦截记录甚至冻结欺诈者的账号。第三类措施是借助数据库和反欺诈模型审核互联网金融平台的用户资料，提前阻止黑名单和高风险用户的金融服务申请，并利用核心算法对所有用户进行风险评估。

3. 事后溯源——数据挖掘

对于已经发生的欺诈事件，企业可以利用相关日志溯源，挖掘整个犯罪过程，帮助同业及时预警，防范更多欺诈事件的发生。企业在互联网环境中面对的威胁对手不再是各自为营的攻击者，更多的是分工明确、协同合作、深度隐蔽的黑产团伙。为了能够从相关威胁信息中挖掘出隐藏在其背后的黑产团体，基于知识图谱的黑产特征挖掘方法被提出，将知识图谱思想和机

器学习算法结合，以恶意欺诈账户为分析源，从多个维度挖掘关系属性，实现多源数据融合建模，并利用算法智能识别强关联账户，从复杂的数据关联中汇总梳理发现隐藏关系，进而暴露黑产团伙。

二、数字金融反欺诈面临挑战不断升级

金融欺诈手段随数字化技术的进展不断升级。金融欺诈方式从传统的盗号、盗刷等简单手段逐渐演变为现时的高度场景化行为，数字化金融欺诈渗透的业务环节多，手段新颖，具有很强的隐蔽性及危害性。数字金融欺诈的目标也从一家公司到多家公司进而扩展到多个行业。因此，反欺诈系统一方面需要各公司各行业的联动，相互之间增强数据、内容的交流和共享，打破屏障；另一方面也有赖监管部门联合治理，持续健全完善管控体系。

（一）数字金融欺诈场景不断增多

1. 数字金融欺诈行为呈现场景化

常见的数字金融欺诈场景有网络借贷、网络支付、消费金融和供应链金融等。**在网络借贷场景**，账户注册阶段，欺诈者采用伪造身份注册、冒用他人身份注册、自动化垃圾注册等手段完成注册；在账户登录阶段，欺诈者的金融账号往往存在盗用、冒用、异常共享等行为；在贷款申请阶段，欺诈者通过提供虚假申请信息获得超额贷款；在还款阶段，欺诈者可能恶意拖欠，或利用非法取得的他人信用卡进行欺诈性交易。**在网络支付场景**，黑色产业团伙往往通过社会工程学方式与技术手段，如虚假 WiFi、病毒二维码、盗版 APP 客户端以及木马链接等，盗取个人姓名、手机号码、身份证号码和银行卡号等直接关系账户安全的要素信息，用于精准诈骗、恶意营销。**在消费金融场景**，诈骗套现行为可能发生在账户注册、激活、登录、交易、信息修改等环节。**在供应链金融场景**，供应链金融欺诈就是企业将虚假交易数据与虚构经营数据，作为供应链授信的依据。

2. 数字金融欺诈受害群体逐渐年轻化

受新冠肺炎疫情影响，2020 年线上活跃用户数量和用户活跃时长均创下历史新高，在线办公、居家上课、网络购物等成为重要的办公、学习和生活方式，给欺诈分子扩大用户接触面、升级诈骗手法套路提供可乘之机，致使数字诈骗风险呈上升态势。

从 2020 年的数据可以看出，受骗用户中“90 后”年轻人已经成为诈骗分

子的重点诈骗对象，受骗数量超过其他年龄段人数的总和，占比达 63.7%；其次分别为“80 后”、“70 后”，分别占比 19.6%、8.1%；值得关注的是，“00 后”受骗用户数量也在上升，占比达到 4.3%，进一步反映出诈骗分子的欺诈目标正逐步向熟悉互联网但风险防范意识较差的年轻群体转移。

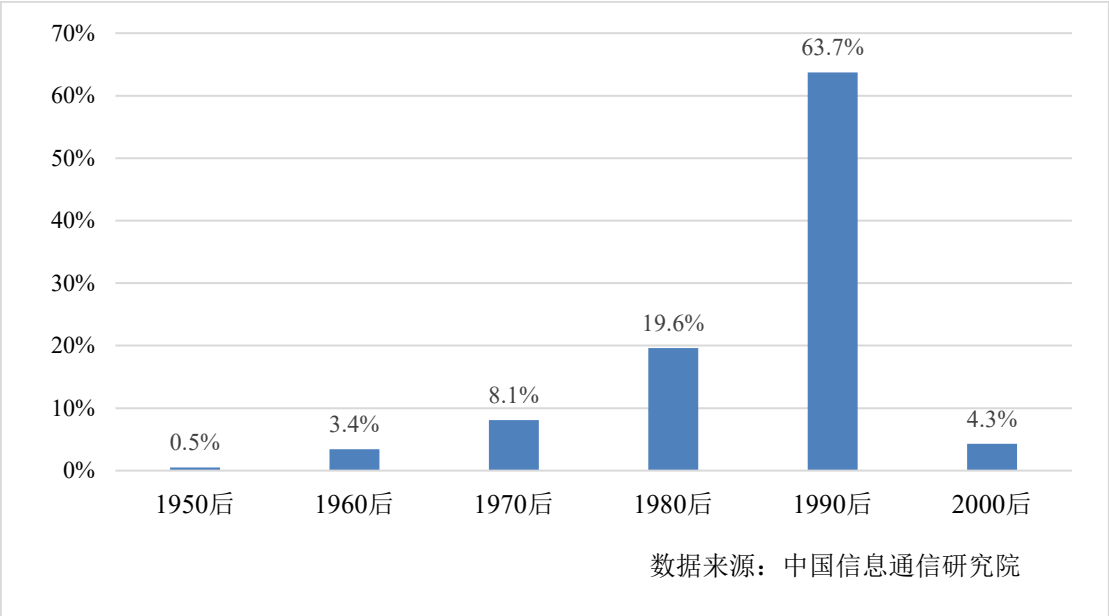

图 1 受骗用户年龄占比情况

（二）数字金融欺诈产业链更加成熟

1. 数字金融欺诈手段快速变化

根据公安部数据统计，数字金融欺诈手段快速发展，目前已经形成了互联网社交软件诈骗、车票机票退改签诈骗、虚假购物消费诈骗、虚假网站和链接诈骗等至少 18 类诈骗手段，并且诈骗手段仍在持续快速更新和发展。仅在 2018 年，网上信用卡诈骗、网上购物退款诈骗及利用社交平台伪造身份诈骗等诈骗案件共立案 38.6 万起，占网络诈骗案件总数的 61.8%（公安部数据）。

截至目前，科技欺诈手段呈现以下七种发展趋势。**一是覆盖面更广。**犯罪分子在实施犯罪的过程中通过电话、短信、社交平台、网络等手段，地毯式发布虚假信息，造成较大范围的损害。**二是手段更新更快。**诈骗分子的犯罪手段层出不穷，从一开始只是利用冒充电话、虚假中奖短信等简单手段实

施犯罪，到现在，通过互联网网站、网络链接、手机病毒、二维码等高科技手段实施犯罪。**三是反侦查能力更强。**在诈骗案件中，犯罪团伙往往有细致的分工，并且采取远程的非接触式的诈骗，根据犯罪需要分饰不同角色、承担不同的分工，例如有专人购买手机通讯工具，还有专门负责与受害人进行通话的话务员，各项程序的负责人甚至互不相识，都受幕后操纵者指挥。**四是隐蔽更深。**随着国内打击力度加大，部分犯罪分子隐匿在国外，租用服务器通过网络、电话对国内群众实施诈骗，一旦被公安机关追查，因其在国外往往能够轻易脱身，从而逃避打击。**五是抓捕难度更大。**黑产团伙逐渐向专业化、集团化方向发展，黑产团伙内部分工明确，职能划分清晰，各组织间互不认识，只通过线上联系，核心成员利用远程操作、不定期更换窝点等手段摆脱执法机构的追踪和抓捕，使得执法机构难以全链条打击和抓捕。**六是追赃更难。**诈骗分子在成功骗取资金后，会在短时间内快速通过多种途径进行“洗钱”，给追讨诈骗资金增加较大难度。**七是无法除“根”。**由于犯罪团伙内部分工明确，且不同环节人员之间互不认识，各环节间保持单线联系，执法机构在打击过程中，很难对欺诈团伙核心成员进行有效打击和抓捕，无法完全清除诈骗团伙。

面对发展迅猛的黑产团伙和黑产技术，金融反欺诈行动和技术都面临空前巨大的压力。需要有关部门持续加强大数据、云计算、区块链等新技术在反欺诈领域的运用，提高跨行业、跨市场交叉性金融风险防控能力，为金融反欺诈提供有力支持。

2. 数字金融欺诈团伙产业分工更加细化

数字金融欺诈属于技术含量高、流程复杂的高智商犯罪，以团伙联手的产业链或供应链方式，使整个作案流程化，构成一定的数字化金融欺诈系统。信息源、协作方、实施方相互合作，彼此交融，涉及欺诈金额巨大，涉案人员众多，形成一条犯罪产业链，造成了严重的不良社会影响。具体而言，数字金融欺诈产业链主要包括诈骗源头、信息贩卖、诈骗实施、资金转移和跑腿分赃五个层次。

数字金融欺诈产业链第一层为诈骗源头。对于当今组织化规模化越来

越强的欺诈团伙来说，各类账号已经成为欺诈的核心资源，各类欺诈工具是欺诈者获取批量收益的基础。欺诈账号的来源主要包含注册和盗号两类渠道。

数字金融欺诈产业链第二层为信息贩卖。个人信息批发商从黑客和线下信息收集者手中购买用户数据，而钓鱼网站批发商则购买木马和钓鱼网站。

数字金融欺诈产业链第三层为诈骗实施。诈骗实施者通过组合资源与基础工具，把所有核心资源串联起来，形成各作恶场景的业务工具，提升作恶效率。

数字金融欺诈产业链第四层为资金转移。诈骗得手后，资金将会转入一个不属于诈骗者名下的银行账户，然后迅速将资金在多个账户中转移并逐步分散至上百个账户内，期间还可能利用第三方支付平台，以此提高警方侦查难度。为了提高安全性，甚至有诈骗团伙通过将资金转移到海外再转回的方式规避监测。多数情况下，由于查询异地银行账户所需的手续复杂，涉及地域多，警方可能会因为追踪成本过高而不得不放弃追踪。

数字金融欺诈产业链第五层为跑腿分赃。跑腿分赃通过提现和各种实物或虚拟价值套利方式进行变现，由于取现等行为会留存身份痕迹，诈骗团伙往往会利用一些跑腿公司实施变现动作，即使欺诈行为被警方破获，在取现、收获环节实施抓捕时也只能控制跑腿公司人员。

3. 数字金融欺诈行踪更加难以锁定

非定点诈骗最大的特点是移动化。随着金融业务不断向移动端迁移，诈骗分子不断将各类热门网络应用作为新型诈骗实施渠道，逐步将单一的电话诈骗扩展为跨平台、跨网络诈骗，其中微信、QQ、APP、网站、支付宝、二维码等各类互联网应用已经成为当前诈骗的主要实施渠道。诈骗分子利用网络环境，不受空间距离的限制，异地甚至异国作案使得反欺诈更为困难。2020 年中国信息通信研究院联合公安机关累计研判处置涉诈域名 2.5 万个，从 IP 接入地情况看，绝大多数为中国大陆以外地区接入，占比超过 95%。

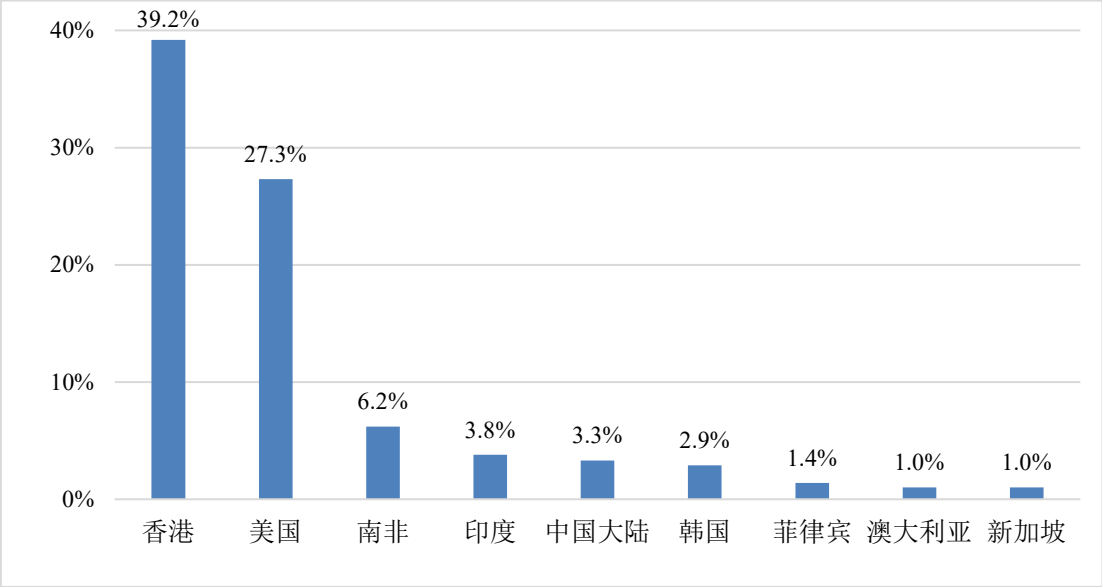

图 2 涉诈域名 IP 接入分布情况

非定点诈骗的另一个特征是诈骗小额化、高频化。单笔欺诈造成的损失多数都在万元以下，然而欺诈次数和规模高速扩张，总损失金额仍然很高。

非定点诈骗的第三个特征是匿迹化。数字化金融欺诈在盗号盗刷、冒用身份的过程中，常利用高科技手段隐匿行踪，依靠传统反欺诈手段很难取证。

4. 数字金融欺诈团伙跨境作案形势严峻

随着国内打击数字金融欺诈的力度加大，部分欺诈团伙窝点逐渐转向境外。2021 年 5 月，公安机关开展“断流”专案行动，通过斩链条、断通道，挖金主、打蛇头，向招募人员赴境外实施电信网络诈骗犯罪发起凌厉攻势。截至 2021 年 10 月，全国公安机关共打掉“3 人以上结伙”非法出境团伙 9419 个，破获刑事案件 4160 起，抓获犯罪嫌疑人 33860 名，其中，组织招募者 931 名，运送接应者等黑灰产人员 913 名，非法出境人员 32016 名，串并破获电诈案件 1021 起，挖出境外电诈窝点 100 个、金主 82 名。

（三）数字金融反欺诈需要多机构跨领域合作

各金融机构和类金融机构在反欺诈领域取得一定成果的同时，问题也在不断显现，各机构对金融反欺诈的认识程度和技术能力不同，机构间反欺诈水平差异较大，跨领域合作还需要进一步深入。跨领域合作对于金融欺诈

的直接关联机构至关重要，商业银行、支付机构和其他有关各方不仅要从技术层面加以提升，还应从跨界合作、法制建设等方面完善配套措施。数字金融反欺诈必须走向联合打击。

从实践经验来看，反欺诈之战不是某一种技术或方法的单打独斗，而是一场集数据、技术和机制于一体的综合防御战，数据是反欺诈体系建设的核心和前提，技术是打赢反欺诈之战的重要支撑，机制是优化反欺诈效果、提升反欺诈能力的重要保障。从数字金融反欺诈的实施主体和手段来看，某一主体的反欺诈需要其他主体的配合与多种技术手段的综合运用，需要跨领域合作才能发现欺诈的真面目，才能彻底铲除黑产团伙。

（四）数字金融反欺诈法律和监管体系不断完善

互联网科学技术不断发展，诈骗分子也充分借助网络技术进行金融欺诈，并愈来愈嚣张。针对如此严峻的形势，各地区按照国务院的部署和要求，联合当地公安部门、通信管理部门、银行监管部门、宣传部门等部门形成多方联席会议制度进行专项治理，初步建立了自上而下的治理体系。

2016 年 11 月 7 日全国人大表决通过了《中华人民共和国网络安全法》，该法律规定了网络数据安全、网络信息安全等方面的法律条例，切实保障了网络信息安全，更为打击数字金融诈骗打下了坚实的基础。法律规定相关的网络产品提供商应注重网络数据的安全性，特别是要采取各种措施来维持网络用户各种信息的安全。该法律还为网络服务提供商和数据持有者与公安机关合作调查违法犯罪和非法提供数据做出了更为细致的指示。除此之外，我国在《中华人民共和国刑法修正案（九）》中增加了相关人员和单位利用互联网实施违法犯罪活动的刑事责任。

工业和信息化部作为电信行业监管部门，通过行政命令、政策性指标和相关行政法律法规来引导和制约相关企业。通过统筹黑卡专项治理行动，对涉及三大运营商的黑卡治理方案进行监督；大力实行的网络电信用户实名化，解决了因网络电信虚拟性和不确定性导致的网络电信诈骗行为的追踪和追责遇到的难题。

市场监督管理局作为市场监督部门，定期检查运营商的实名制执行情

况，通过行政处罚、责令整改等方式，起到监督震慑作用。

公安部作为监管和执法部门，通过建立“侦查打击、重点整治、防范治理”三位一体的执法体系来打击金融欺诈犯罪行为。公安机关部署了专门的力量，扎实开展了网络诈骗犯罪打击专项活动，积极邀请相关专家分析讨论案件，并利用媒体平台来向大众宣传防诈骗的知识，通过这些措施取得了较好的成效，有力地遏制了电信诈骗逐渐扩大的趋势。

三、新技术在数字金融反欺诈中的应用逐渐成熟

（一）大数据和云计算技术

1. 资源整合

依托大数据、云计算相关技术，将海量数据源进行汇总整合，消除不同地域、不同领域、不同部门间资源无法共享的隔阂，取长补短，实现资源与数据的充分利用。资源整合主要包括数据资源与计算资源两种形式的整合。数据资源的整合包括对海量不同数据源的捕捉汇总，寻找不同数据之间的关联性，进行合理的存储结构设计，按照预先设定好的主题与维度结构化存储，实现数据规范化；计算资源整合主要体现在以云计算技术为主体，以分布式计算、效用计算、负载均衡、并行计算、网络存储、热备份冗杂和虚拟化等计算机技术为辅助手段，实现对计算资源的合理分配，保证系统的稳定。

2. 数据预警

依托现有大数据技术的资源整合能力，做到海量数据实时捕捉、实时计算，及时发现风险并做出预警。数据预警系统的作用主要体现在合理的数据资源和计算资源整合后，充分有效地利用服务器资源，将海量数据实时计算的压力分摊减小，使得系统可以在最短的时间内，针对即时发生的行为数据做出决策，分批次、分阶段生产预警信息，使得场景不再局限于单纯的流式计算，实现微批处理的实时性，并在实时计算中，加入复杂的关联条件，使得决策信息多样化，显著提高预警精准性。

3. 数据模型

精准而科学的数据模型需要强大的基础数据积累与优质的资源整合。在基础数据积累方面，由于反欺诈场景的多样性与复杂性，单一的反欺诈模型应对不同的欺诈场景处理能力有限。因此，应结合实时数据和非实时数据两种方式对客户行为进行采集，其中，实时数据主要针对客户单一交易行为进行预警，非实时数据主要针对客户一段时间内累积的历史交易情况进行预警。在优质资源整合方面，基于面向主题的数据仓库对采集数据进行存储，

将海量数据组织汇总为较高层次的主题，将相关主题集成归并为主题域，实现对数据的高效操作与处理。依托于优质的计算资源实现强大的分析计算能力，构造针对不同场景的海量模型，同时将海量模型集成整合，形成一个完善而科学的反欺诈数据模型系统。系统以数据模型为反欺诈分析中枢，结合数据预警系统的实时反馈，帮助模型持续优化，让模型具有不间断的自主学习、自主迭代、自主判断能力，使其成为反欺诈场景中最坚实的核心。

（二）人工智能技术

应用先进的人工智能技术，以数据为驱动建立智能化的风险预测防控模型，在金融欺诈防控方面有重要应用。AI 在金融交易反欺诈方面，特别是针对信用卡盗刷、APP 转账等欺诈，目标是在不过分打搅客户的情况下，可大大提高欺诈案件识别的覆盖率。在反洗钱方面，目标是用机器学习建模识别出不是洗钱的方法，将其排除，并对洗钱账户进行评分和分类，这样可以根据调查和审核人员不同的能力来分配不同的案件，帮助他们提高效率。

根据《“十四五”规划纲要和 2035 年远景目标纲要》，“十四五”期间，我国新一代人工智能产业将着重构建开源算法平台，并在学习推理与决策、图像图形等重点领域进行创新。我国人工智能技术创新处于前所未有的活跃期，人工智能产业轴心从前沿技术向行业应用转变。人工智能和各产业深度融合，未来将形成人工智能产业集群，反欺诈产业链将成为人工智能的一个重要应用场景。

（三）区块链技术

1. 重构信用机制

区块链技术实现了信用创造机制的重构，因而从事前预防层面上减少数字金融欺诈的可能。在金融交易系统中，一般通过算法为人们创造信用，从而完成双方信任的过程。

一方面，区块链的技术特性保证了系统内部价值交换过程中的行为记录、传输、存储的结果具有不可篡改的特性，同时，其信息溯源能力使业务中交易信息、资金来源、资产信息等数据具有透明、可追溯特性，从而大幅

度提升了信用体系的准确性和有效性。

另一方面，通过区块链智能合约技术，交易双方甚至无需了解对方基本信息，也无需借助第三方机构的担保，可以直接进行可信任的价值交换，大大减少交易过程中欺诈发生的可能性。

2. 保护个人隐私

数字金融欺诈黑产中重要的一个环节是非法获取用户个人隐私信息，包括身份证信息、账号密码信息、银行卡信息等。随着金融业务与信息技术的不断融合，用户身份识别和安全认证一直是金融反欺诈过程中面临的重要问题。

区块链技术通过基于节点的授权机制，保证了用户控制的隐私权限设计中的私密性和匿名性，只有授权节点才有相应权限查阅和修改有关数据信息。因此，在完善用户个人信息保护制度、保证个人财产状况和信用状况等私密信息安全领域上，区块链技术具有重要应用价值。在区块链技术的赋能下，个人数据安全将被极大地加强，进而大幅增加欺诈黑产非法获取个人信息的难度，减少金融欺诈的发生。

3. 共享行业信息

区块链可以通过打通数据孤岛，建立更加公开透明的金融业务环境，减少欺诈行为，赋能监管执法机构打击犯罪黑产。

区块链因其具备了匿名保护、安全通信、多方维护和可溯源等特点，其多方分布式记账的模式保证数据对所有参与方都是可见并一致的，实现了数据多方共享的特性，有助于进一步打破数据孤岛的现状。在金融业务开展的同时及时将交易信息同步上链，可实现交易信息的公开透明和可溯源，同时节省了金融场景中多方信息不对称导致的额外工作（如数据传输、结算对账、人工核实等）的开销，从而有效降低资金成本和系统性风险。

在此基础上，由于多方维护共同的信息账本可有助于实现行业信息的共享，从而有助于监管部门和合规部门动态掌握交易的全貌，实现对目标数据的实时或准实时获取，在打击多头借贷、骗保、票据作假、重复质押等方

面起到积极作用。

（四）物联网技术

物联网技术作为一项赋能技术，提供对各种类型主体的动态、高效监控感知、状态获取的能力。在数字金融反欺诈应用中，物联网技术可以帮助实现对金融主体相关信息动态的多维度、全天候的收集获取，特别是在 5G 技术加持下，可以实时掌握主体的各类信息，这就奠定了以主动识别为核心要求的新型监管模式的基础能力。在金融反欺诈的过程中，面对日益复杂的金融市场行为和交易体系，除了传统的金融层面数据，通过物联网+5G 获取和感知其他相关数据，有助于实现主动识别和提前预警。

强化跟踪分析能力，提升金融反欺诈精准度。未来物联网将广泛应用于国民经济各行各业，很多重要的资产或设备数据将及时反映金融活动的现状和趋势，成为金融反欺诈的决策依据。基于统一、泛在、互联的物联网，可以实时掌握各类应用数据，实现对金融反欺诈的整体把控。

物联网+5G 应用带来的多维度数据，实现企业生产运营全过程监控。物联网+5G 技术广泛应用于工业制造领域，通过各类摄像头、传感器，实现对企业生产经营全过程、以及对各类押品、工程建设的实时感知，完成对于分散性、多业务资金流向的统一化和穿透式监管，解决传统监管手段在分散信息获取、业务动态跟踪等方面的瓶颈。

四、数字金融反欺诈的应用场景分析

（一）数字金融反欺诈在银行业的应用

在金融科技带来的创新驱动下，银行正在转型为智慧银行、开放银行、生态银行。数字化银行的大潮下，银行业务模式更加灵活、开放，在为客户提供更加优质服务体验的同时，也成为网络黑产的重灾区。数字金融反欺诈一直是各商业银行的重点工作，新型风控技术正在全面应用于数字金融反欺诈各个阶段。

一是事前阶段，通过引入新型身份认证技术手段，强化金融业务健壮性。随着金融业务的快速发展，例如 U 盾、密码器等传统认证手段，其安全性较强，但使用方法相对繁琐，易用性不高，逐渐导致产品易用性和安全性出现不平衡的情况。通过建立交易认证安全基线，并引入设备指纹[1]、手机网关[2]等身份认证增强技术，提升金融业务易用性，规范各认证手段使用场景，强化金融业务对欺诈的抵御能力。

二是事中阶段，使用涵盖多渠道的新型风控模型，加强实时风控。转账汇款业务作为最常见的银行基础业务，也是欺诈高发业务场景，涉及柜面、ATM、智能终端、网银和手机银行等多种渠道及多个业务部门，银行各部门积极沟通，逐一对各渠道业务流程展开细致调研，共同研究制订流程改造方案和系统拦截策略，实现欺诈账号的系统对接和自动拦截。建立欺诈风险管理平台，与业务系统自动化对接，形成全渠道、全天候、7×24 小时的电信欺诈事中防控体系，对转账汇款交易进行实时筛查和预警控制。

三是事后阶段，深化警银信息合作，共建联控机制。银行以欺诈账号为切入点，通过与公安机关的信息交互，建立总对总及区域层面的欺诈账号共享合作机制，为全国范围内欺诈账号收集和联控联防奠定良好的基础。

（二）数字金融反欺诈在保险业中的应用

保险欺诈形式多样，分布广泛，机动车险、企业财产险、货运险、健康

[1] 设备指纹是一组设备固有的、较难篡改的的属性或特征，作为设备的唯一标识，防止被篡改或仿冒。

[2] 手机网关认证是基于运营商移动数据网络进行身份认证的方法，由运营商通过数据网关对客户的 SIM 卡进行识别，检验是否使用本机号码进行业务交易。

险、农业保险等多个险种都屡屡报出欺诈案件。保险欺诈具有很深的隐蔽性，并且数量和金额也在不断地攀升，各类新型欺诈形式层出不穷，欺诈手段频频升级，在给保险公司带来巨额损失的同时，也损害了投保人的正常权益。保险市场上的双方都面临信息不对称，这为欺诈分子创造了可乘之机。我国保险业反欺诈进展可以从以下三个方面来概括。

一是建立保险行业协会行业信息共享平台。中国保险行业协会（以下简称“中保协”）依托车辆保险信息集中平台项目设立保险行业信息公司，逐步发展建设全国行业信息平台。目前，中保协已组织各家保险公司就意外险、健康险投保信息与理赔信息与中保信平台进行对接，实现投保、理赔信息共享。该信息共享平台可有效减少虚假赔案、提高承保质量，对于提升行业信息化水平、防范保险欺诈也有战略性意义。

二是各机构设立反欺诈部门。目前，基本每家保险公司都会设有专门的反欺诈部门，反欺诈部门的职能是制定公司反欺诈指导文件，对承保业务进行反欺诈的理论研究和实地调研，严厉打击保险欺诈行为，推动公司反欺诈信息技术和制度建设。对于涉嫌欺诈的案件，联合调查公司进行调查取证。制定反欺诈策略，定期分析欺诈数据，汇总上报行业协会。

三是各机构加强技术研究。我国保险反欺诈的技术手段已经从最初的人工检测发展到现在的黑白名单、规则引擎等先进技术手段。所谓黑白名单是指保险公司的承保系统会关联反欺诈系统。反欺诈系统设置了一些指标，比如“法院失信名单”、“法院执行名单”、“犯罪通缉名单”、“欠税单”、“信贷逾期名单”等诸如此类的筛选项，指标由保险公司风控部门进行设定，并赋予相应权重。若投保客户的身份信息上述指标项或者综合得分较低，保险公司将拒绝承保。

（三）数字金融反欺诈在证券业中的应用

将文本挖掘、数据挖掘、人工智能等技术应用于反欺诈实践，证券交易所开发出大数据监察系统、上市公司监管系统、风险监测监控系统，不断提升金融科技监管能力，打击证券违法违规交易。其中，大数据监察系统具有高频时间序列匹配、交易重演、多维度分析等功能，并先后上线了“老鼠仓

智能识别”、“内幕交易智能识别”和“市场操纵智能筛查”等大数据应用系统，通过将投资者委托、成交、托管等交易数据，上市公司董事、股东、企业管理人员、中介机构等相关知情人士的资料，以及上市公司公布的重大信息等内容进行关联分析，并与各类违规交易分析模型进行比对，实现精确甄别异常交易、内幕交易、市场操纵、老鼠仓等违法违规行为。

五、数字金融反欺诈发展建议

（一）国家层面

1. 细化数据要素流动法规要求

《网络安全法》、《数据安全法》、《个人信息保护法》等数据安全方面法律法规不断出台、完善，国家对数据的监管逐渐清晰，但操作层面指导数据要素有序流动的具体监管办法、技术标准等还有待进一步细化。数据要素的合理利用与依法有序流动，是金融行业数字化转型、有效防范化解金融风险的关键手段，数据要素作为对抗欺诈团伙的基石，未来需要加速数据要素相关法规的细化，一是加快厘清数据归属权和使用权；二是探索适应数据要素市场化流转的机制和技术基础，加快多层次数据交易市场；三是大型金融机构先行开展金融领域数据要素市场化试点。

2. 加强国际间反欺诈合作

随着我国金融市场对外开放的态势逐渐深化，金融领域跨境监管面临新的挑战。首先，不同国家的金融市场成熟度不同，相关规章制度也存在着一定的差异。其次，跨境交易的反欺诈监管策略有可能会出现监管套利的情况，这也是对监管有效性的挑战。三是，当今国际关系变幻莫测，因国家间的摩擦有可能导致监管机构间缺乏稳定、长效的合作。在此背景下，中国境内外欺诈犯罪分子相互勾结，作案手段智能化、高科技化情况日益严重。因此，在处理跨境欺诈犯罪时，应注重加强国际间合作。例如，在信用卡领域，与信用行业欺诈规避组织（CIFAS）开展合作，通过高科技技术和组成联盟的形式，发现、预防和阻止社会上的欺诈行为。此外，可在可控程度内接入大数据信息平台，实现国际的联防联控，减少犯罪分子使用相同手法作案，打破跨国壁垒，提高反欺诈效率。

3. 聚焦反欺诈关键技术，集合产、学、研力量开展攻关

金融反欺诈离不开数据驱动，同海量的正常数据相比，欺诈数据在可用数量和质量上都存在较大差距，数据不均衡已成为制约反欺诈数据分析的重要因素，需要国家加强对金融数据反欺诈技术领域的引导和支持，进一步提升欺诈样本匮乏场景下的反欺诈能力。为此，一方面建议引导社会力量及

科研中坚投入到小样本数据反欺诈的研究工作中，加大对半监督学习、无监督学习等小样本分析技术的科学研究力度，通过产学研合作模式加速科研成果的应用与转化，促进小样本反欺诈技术发展，提升小样本反欺诈能力成熟度；另一方面建议建立国家级反欺诈数据平台，构建统一的标准数据体系，为数据共享、复杂分析、自动决策等提供数据支持，加速提升反欺诈数据分析能力。

（二）行业层面

1. 积极推动各机构、行业反欺诈联动

数字金融欺诈具有跨部门复杂性、跨区域高发性和跨行业隐蔽性等新特点，对反欺诈提出了更高的要求，客观上需要政府和行业监管部门、金融机构、科技企业以及行业协会等市场主体形成联防联控的生态联盟，反欺诈方式从单个企业的孤军奋战走向跨行业、跨企业的协同作战。通过筹建数字金融反欺诈联盟等行业组织，搭建起数字金融反欺诈协同治理的新平台，能够有效整合政府和社会机构的力量，推进欺诈案件的信息共享、数据共享，建立全方位反欺诈联防和信息互通机制，及时识别和预警数字金融欺诈风险，不断加强欺诈的风险管理，共建金融安全生态圈。

2. 加强重点人群反欺诈宣传教育

针对重点人群，应当加强金融欺诈常识普及，培养反欺诈意识。一是普及数字金融相关法律常识，对诈骗分子在欺诈过程中常用的诈骗手法，明确指出其中的漏洞与风险，讲明其中的利害关系。二是加大数字金融欺诈案例宣传，邀请专业数字金融领域从业人员，普及数字金融基础知识，针对当前诈骗分子常用的诈骗手段进行剖析讲解，模拟诈骗情景，提高群众对于欺诈行为的辨识度。三是多样化宣传手段，紧密贴近日常生活，充分考虑大众对于教育方式的接受度，不搞刻板化、枯燥式教育，结合当前时事热点，将反欺诈知识在日常生活中自然普及，同时，有效地调动受教育者的积极性，起到一人学习、全家普及的效果。

（三）机构层面

1. 筑牢业务安全基线

随着近年来外部威胁的持续加大，以及数字金融技术的加速创新，业务面临的安全威胁愈发凸显。在此背景下，由于业务场景安全策略与业务风险防护需求缺少统一的标准，导致很多数字金融业务的安全策略与实际需求不匹配，出现安全短板或防护过度的情况。为此需要面向各类交易场景体系化设定防控基线，系统化对安全防护策略及业务风险等级进行量化评估，体系化地做好身份识别、涉账交易等重要环节的安全控制，把握业务交易和安全的平衡。

2. 加强隐私计算等技术创新和应用

随着黑产行业的智能化与集团化，各类欺诈手段的特征越发隐蔽，跨行业欺诈逐渐成为常态，单次欺诈行为贯穿社交媒体、银行多个环节，各机构基于自身数据已疲于应对，所以连续、一致的数据流对于整个反欺诈系统的成功运行至关重要。随着国内针对数据安全的监管不断加强，加上金融业数据具有高价值高、强隐私等特性，相关数据不能轻易对外开放。加强隐私计算等技术创新和应用，可以帮助金融相关机构在不泄露客户个人信息及模型资产的前提下，提供联合数据挖掘及建模条件，实现在保证数据隐私和安全的前提下共享数据价值，共同进行数字金融欺诈防护。

3. 加强专业人才体系化培养

传统的反欺诈团队已经不能适应新形势，当前威胁形势下，金融机构更需要技术业务兼顾的复合型人才，如大数据人才、黑产防护技术人才、安全建模人才等。为此，需要加强企业内对技术型人才的培养提升：一是需要加强对技术人才的学习培养，定期安排安全人员与互联网、行业头部企业等优秀机构进行技术交流，学习掌握最前沿的技术应用；二是以技术能力为导向，在内部建立安全攻防及反欺诈人员的岗位能力体系，鼓励安全人员参与新兴、前沿技术的测试研究；三是鼓励创新，建立奖励机制。鼓励和引导行业从业人员积极探索利用人工智能等新技术解决数字金融欺诈治理的重点难点问题，对取得较好治理成效和社会效益的项目进行一定的奖励并推动其在行业内的推广应用。

附录：数字金融反欺诈的应用案例

为展现目前金融科技前沿技术的应用情况，本报告筛选出七个具有代表性的案例以飨读者。从不同技术和应用场景对新一代数字信息技术在金融反欺诈中的应用进行了分析[3]。本附录所选案例由中国信息通信研究院云计算与大数据研究所金融科技部通过公开渠道征集，由案例公司独立完成，版权属于各案例公司，与本报告编写单位无关。

（一）AI 反洗钱技术应用

1. 案例简介

保留传统反洗钱系统的原有优势，充分运用专家经验，利用机器学习、知识图谱、数据挖掘、大数据等新兴技术，对反洗钱系统进行智能化改造，充分挖掘数据价值，提高反洗钱系统的监测效率，有效打击犯罪。构建的 AI 反洗钱系统与传统反洗钱系统相比，保持 100%专家审核结果全部命中的同时，最高有 98%的误报率降低，极大地提高了行内反洗钱业务专家的审核效率。

2. 解决的难点问题

（1）利用机器学习技术，并结合专家规则，形成丰富且自适应的模型触发模式。

（2）针对多种类型数据，结合静态数据，利用多种模型保证检测效率。

（3）利用大数据平台和图计算技术，发现复杂洗钱行为。

（4）引入了知识图谱技术，构建直观展示方式。

3. 创新技术和应用

案例中所构建的智能化反洗钱监测模型是反洗钱场景下的应用， 具有以下几个创新点：

（1）利用多种类型的机器学习模型应用于不同数据的情况

[3] 本报告案例呈现的观点仅代表案例提供单位的观点，不代表本报告编写单位的观点。

首先，系统会对数据进行一系列数据预处理，得到标准的、干净的、连续的数据，提供给数据统计、数据挖掘等使用。其次，系统在借鉴专家经验统计得到的规则形成普通特征的基础上，利用这些特征的组合生成更高级特征，表达更加丰富的信息。

（2）构造交易知识图谱发现社群关系，监测异常行为

本案例在系统中引入知识图谱、图计算、图神经网络技术来发掘复杂关系网络。首先通过利用多个途径的数据，来构建交易知识图谱合理表示交易关系。之后利用最短路径法等图计算方法计算得到整个网络中具有特定结构的关系网络。之后，进一步引入了图神经网络，发掘带有属性的特殊社群结构。通过以上方法，再对整个案件中涉及到的转账、取现、查询等多种事件进行结合考虑，就能全局性地掌握案件动向。之后将基于规则的图谱典型特征、高级特征和基于知识图谱的关系信息想结合，共同作用、参与到多模型的机器学习监测过程中，得到精确结果。

（3）利用多模型融合和自学习机制来提高异常行为检测效率

整个智能化机器学习流程使用了多种模型，在这些模型的共同作用下，得出高准确性的可疑交易监测结果。此外模型会随着专家审核数据的积累，不断更新数据到输入阶段，并制定了相应策略，满足条件时不断的根据新增专家数据自动学习更新模型，以及时利用专家分析结果数据，得到更准确结果。

（案例提供单位：神州数码信息服务股份有限公司）

（二）无监督机器学习赋能银行反洗钱方案优化升级

1. 案例简介

某头部股份制商业银行在对公账户发起的支付交易和跨行转账交易场景下，存在资金交易频繁、金额较大、过渡性质明显、与客户身份不符的疑似洗钱交易行为。然而，受限于行内现有规则检测覆盖范围窄、曾试用的无监督机器学习算法难以落地应用等因素，现亟需一套全新解决方案。本案例

搭建了无监督可疑公转私交易监测模型。该模型基于无监督机器学习算法，配以建模工具 dCube，与行内现有专家规则引擎及有监督机器学习高效融合，实现对于已知欺诈及未知欺诈的全面捕捉，优化升级行内现有系统。

2. 解决的难点问题

本案例中，一站式无监督建模工具 dCube 是较为专业的无监督算法建模工具，在内置了专利算法的同时，又支持了特征处理及模型的优化。同时，本案例的建模工具能够在短时间内完成部署、与行内现有检测体系高效融合，实现多业务场景并行计算、大规模交易数据检测并实时反馈信息，确保准确率。

3. 创新技术和应用

以无监督机器学习算法为核心的解决方案，不仅成功落地金融反洗钱领域，亦顺利应用于包括金融交易、信用卡申请反套现在内的诸多场景。

以申请反欺诈场景为例，助力美国领先的信用卡发行商，减少因信用卡申请欺诈产生的经济损失。通过迅速部署以无监督机器学习算法为核心的解决方案，帮助客户检测原有方案所遗漏的欺诈行为、提前捕获团伙性和未知性欺诈攻击、降低误报率并实现对整个欺诈团伙的批量决策、提高运营效率。基于解决方案，客户的欺诈检测增益率高达 25%、检测准确度高达 94%、误报率低至 0.17%并挽回远超千万美元经济损失。

无监督机器学习专利算法不依赖于额外数据，利用有限的数据从而获取重要信息。无监督机器学习用算法和技术为数据补位，能够有效地为客户风控版图提供重要补充。先进的特征工程可以高效地从原始数据中萃取有价值的信息，dCube 风控管理模型能够不依赖数据标签进行具有预见性的决策分析，在保护用户数据隐私安全的前提下做好风控，与当下监管要求的日趋完善以及行业的逐步规范不谋而合。

（案例提供单位：北京维择科技有限公司）

（三）数字金融反欺诈技术在私募基金行业的应用

1. 案例简介

广东省地方金融风险监测防控中心初步建成全国首个专门应用于私募基金行业领域、集“促发展+防风险”功能于一体的私募基金数字化线上综合服务平台——私募基金瞭望塔系统。在反欺诈等风险防控方面，该系统监测范围覆盖已备案私募管理人和未备案私募机构，基于多维度监管、穿透式监管、可视化监管和行为监管四大原则，基本实现了全方位、动态化私募风险监测。

该技术手段主要聚焦行为监管，压缩监管真空，对主体的行为活动进行动态跟踪和多维度、全流程监测，其在识别违法违规从事业务的企业方面具有显著的应用效果。此外，还可应用于非法金融活动的识别和预警，主要表现在通过机器学习等方式对存在风险行为的企业样本进行不断学习，归类形成某类非法金融活动的特征，并建立识别策略，进一步挖掘出开展相同或类似非法金融活动的企业。

2. 解决的难点问题

本案例主要解决了私募行业领域金融风险隐蔽性强、传播速度快、难以打早打小的痛点，以及没有有效监控手段等实际困难，有效帮助监管部门由“手工监管”向“科技化监管”、“事后监管”向“提前发现”、“粗放式检查”向“精细化监管”、“精准监管”转变，深化科技对监管的积极推动，实现对私募行业领域金融风险状况的持续监控和动态分析，极大地提升监管效率。

3. 创新技术和应用

（1）首次实现私募基金领域“募-投-管-退”全流程覆盖

运用基于超资源融合的云计算体系的构造方法，通过云操作的形式语义化和过程的纵横交错化，实现独立分布的超资源间的连接、组合、集成、通信、数据采集、数据更新，连接“伪私募”机构“募-投-管-退”各环节，最终

达到风险识别贯穿业务全流程的效果。综合运用用户画像技术和行为识别技术，采取可视化方式全面整合机构的异常行为和信息，跟踪并描绘机构在宣传和“募-投-管-退”全流程的动态。

（2）首次实现私募基金领域政务数据、机构数据和市场数据融合应用

通过大数据处理流程的执行计划生成方法，采集工商、司法、法院、公安、信访等政务信息、金融机构报送信息及网络负面舆情、投诉信息等数据，对每个数据采集终端匹配独立且唯一的数据传输路径，保证大数据处理过程中的统一性和对比关联性，首次在私募基金领域实现政务数据、机构数据和市场数据等多维度数据的全方位融合应用。

一方面，结合知识图谱技术，描绘股权、司法、业务合作等企业关联关系全景图。另一方面，运用风险和行为等自主识别技术，一是识别产品投向标的属于工商状态为吊销、注销或存在无法联系等异常信息的公司，二是识别是否存在将募集资金投向关联企业进行自融的风险，三是甄别未备案但疑似从事私募业务的机构。

（案例提供单位：广东省地方金融风险监测防控中心）

（四）人工智能助力商业银行提升风控和智能化水平

1. 案例简介

借助数据科学平台 Sophon Base、知识图谱平台 Sophon KG、实时决策引擎 FIDE，某商业银行人工智能与建模团队完成了反洗钱机器学习模型的开发和上线。模型对可疑上报案例的识别精准率较原有的反洗钱规则有大幅度提升，模型预测的洗钱可疑概率前 20%的名单即可覆盖超过 85%的上报案例，预测概率前 30%的洗钱可疑名单错误率低于 7%，且可基本排除反洗钱规则中 60%的预警客户，大幅降低误报率，缩小反洗钱审查范围，大幅减少人工排查确认工作量，降低反洗钱成本，提升反洗钱监测的效率和准确性。

2. 解决的难点问题

本案例开发的模型主要解决了之前模型存在的如下问题：（1）上线部署困难、时效性差；（2）模型重复建设、烟囱化严重；（3）缺乏模型后期监控、更新与维护等问题。

3. 创新技术和应用

在此案例中构建的反欺诈和智能化风控模型帮助银行形成了全渠道的立体防范，并结合实时流处理引擎和实时决策引擎实现了模型对于风险事件的实时拦截，为国内银行业少数的从底层数据平台到上层图谱应用的全链路方案的落地项目提供了帮助，具体创新技术如下：

（1）利用机器学习技术补充现有规则，构建平衡用户体验的反欺诈模型

利用行内客户基础数据、交易数据和登录等行为数据，从交易和客户两个维度进行机器学习建模分析。主要运用有监督、无监督、标签传播和图分析等技术，构建反欺诈综合判别矩阵，并补充行方现有反欺诈规则，解决行方全渠道联防联控难，团伙识别难的痛点。并且平衡了用户体验和风控力度。

（2）提供图数据库到知识图谱的全套方案，洞察高危团伙

通过提供分布式图数据库、图谱构建、图谱展示、高性能图网络特征指标计算等全链路的知识图谱工具，并结合实时决策引擎，将该商业银行的离线训练模型上线到生产环境用于线上实时业务的能力，生成了风险管理驾驶舱，实现了从 T+1、T+0 的事后风险管理向实时风险管理的成功跨越。

（3）专家经验+AI 的双轨决策模式，提升智能化风控水平

基于 FIDE 的实时决策引擎，赋予商业银行大数据环境下的实时决策能力，建立以“数据+场景+技术”为核心的数字智能化运营模式。面对高并发的异常或欺诈行为能够做到实时数据实时决策，突破数据 T+1 的技术壁垒，有效提升对风险行为和交易行为的时效性，并结合反欺诈模型和专家经验，实现毫秒级且精准的拦截与告警。

（案例提供单位：星环信息科技（上海）股份有限公司）

（五）基于大数据技术的风险防控平台

1. 案例简介

某银行大数据风险防控平台，依托于落地实施设备指纹系统，风险决策系统，以及数据源管理平台等产品，结合某银行客户设备信息、申请信息等风险防控数据等，实现自动化识别欺诈风险，通过决策引擎自动甄别有效客户群体，提高了精细化风险管理水平。大数据风险防控平台采用线上方式自动审批客户申请，增加了线上风险定价等功能，使用户足不出户就可以享受全流程无断点服务。本平台帮助客户不断强化风险防控能力，逐步实现流程高效化、操作线上化、产品标准化、审批智能化、管理规范化。

2. 解决的难点问题

本案例平台解决的难点问题包括：精准评估用户或企业的还款意愿和能力的问题；对中小企业进行反欺诈监测、信息核验、信用评分等问题；对各业务链条的风险管理问题；“数字+服务+场景”的生态业务模式问题；贷前、贷中、贷后全周期化的风险监控问题等。

3. 创新技术和应用

（1）强化平台核心能力

本案例将设备指纹、关系图谱和工作流引擎引入到反欺诈平台。

（2）全渠道进行反欺诈

基于大数据风险防控平台的强劲计算能力，通过灵活配置规则和模型，对手机银行、开放平台等多渠道数据进行深入挖掘与分析，深度识别个体欺诈行为和团伙欺诈行为。根据不同渠道和不同业务的特点，及时有效的识别和防范欺诈风险。

（3）全流程信贷风控

结合行业应用及三方数据，通过制定相应的欺诈识别策略，建设标准化的客户信用评分模型，有效评估客户的还款意愿和还款能力。根据信贷业务生命周期不同阶段所面临的风险状况差异性提供全流程的风险审批、授信

定价和风险监控处置等决策支持服务，在紧守风险关口的同时提高贷款办理效率。

（4）实时决策智能化

引入外部数据，包括客户基本信息、行为特征、信用情况、社保、公积金、税务等，与内部数据融合，基于海量信息对客户进行实时全面风险评估。面向不同场景构建反欺诈模型、信用评分模型以及额度定价模型，并支持不同业务场景根据自身风险偏好进行个性化的策略制定，从而满足不同的业务发展需要。

（案例提供单位：江苏通付盾科技有限公司）

（六）人工智能技术在“侦图”中的应用

1. 案例简介

利用深度学习技术和数字图像处理技术，以各个应用场景需求为驱动，打造了以深度学习技术为核心的图像审核产品“侦图”。“侦图”产品涉及图像审核各个领域，实现了从图片到视频的全方位 AI 图像审核能力。

2. 解决的难点问题

本平台解决传统人工图像审核所存在的如下难点问题：（1）时效性不足，传统的用户准入无法在事前进行图像审核；（2）工作量巨大，产品线上每天用户上传海量图片，仅依靠运营人员几乎不可能完成排查；（3）审核难度大，审核人员主观意识对审核结果造成巨大影响。

3. 创新技术和应用

“侦图”通过创新不断提升模型应用效果，使人工智能能够真正的服务于企业，为企业降本增效。针对不同场景，“侦图”研发团队都进行了大胆的尝试与革新，利用不同技术手段进行识别。

在证件鉴伪案例中，基于 PS 照的构成特点，采用 TwoStage+双路卷积的检测方案，最后再用 Stacking 策略进行模型融合，保证了整个模型的准

确性和泛化性能。而屏幕翻拍重点在于摩尔纹的识别，采用了多分辨率网络架构，模拟屏幕照缩放中的摩尔纹变化的动态过程，找出与正常图片的差异。

同背景照中介欺诈群组识别是一种无监督识别方案，在提取特征阶段，我们图像特征和业务属性特征的多模态特征融合可以达到此效果。在实际应用中，背景照群组识别率可达 95%。

“侦图”作为业内首个金融级 KYC 证件识别产品，通过大数据模型算法，利用 AI 能力能够实时甄别身份证，营业执照、公章证明等认证材料是否经过篡改，翻拍，复印等情况，有效提升身份审核效率，降低欺诈，伪冒风险。可帮助金融企业响应监管要求，降低人工成本和欺诈损失。

（案例提供单位：天翼电子商务有限公司）

（七）数字金融反欺诈技术助力政务综合服务平台建设

1. 案例简介

某市政务综合金融反欺诈服务平台利用当地人民银行信用信息数据库搭建数据体系，建立前置反欺诈规则策略和授信评分卡模型，进而对自然人和小微企业进行金融授信。实现了智能秒级实时审批、多维度立体化数据决策、征信数据成本最优和差异化客户授信等功能。该政务综合金融反欺诈服务平台提高了贷前审批效率，降低了风险损失。

2. 解决的难点问题

在传统业务模式下，银行内部欺诈管控效率低下，如何提升反欺诈管理效率成为各大银行面临的重要问题。本案例建成的反欺诈平台，能够帮助银行拓展反欺诈工作的深度，挖掘传统人力审查下难以发现的问题，扩大远程监控的覆盖范围，利用专家规则、机器学习和数据挖掘的行业算法模型，最终全面提升银行的反欺诈水平。

针对数据层面所存在的数据孤岛和数据质量不达标的问题，本案例帮助客户搭建了反欺诈数据体系，包括反欺诈指标体系、用户行业指标体系、自然人和企业用户画像指标体系，建立了完整有效的反欺诈专家模型、反欺

诈评分卡和规则，对解决数据层面的问题有显著作用。

3. 创新技术和应用

项目实施过程中，应用了知识图谱和不一致性检验等相关技术，实现对可疑风险的识别与发现。具体的创新技术如下：

（1）动态分析。主要在于分析图结构随着时间变化的趋势和业务人员认定。基于图谱结构的变化对异常动态进行分析。

（2）关联特征提取。主要是基于一些规则和策略从图结构上提取一些特征，这些特征一般是基于 2 度、3 度甚至更多度的搜索所得。

（3）社区发现分析。主要基于无监督的聚类算法，目的在于找出一些距离较近亲密度较高的群体进行聚类分析，从而进一步分析风险性。根据经验对社群或图上的特征进行社群划分，提取一些子图特征（比如一些简单的，平均年龄、平均收入、平均负债、子图最大年龄差等），然后再用逻辑回归和规则对子图进行评分。

（案例提供单位：和美信息（深圳）信息技术股份有限公司）

中国工商银行金融科技研究院安全攻防实验室

地址：北京市海淀区建材城东路16号

邮政编码：100096

联系电话：010-82988313

网址：www.icbc.com.cn

中国信息通信研究院云计算与大数据研究所

地址：北京市海淀区花园北路52号

邮政编码：100191

联系电话：010-62302912

网址：www.caict.ac.cn