顶象
DING XIANG

关联网络 + 反团伙欺诈

白皮书

V 2.1

ABOUT
关于顶象

顶象是一家创新的业务安全公司 帮助客户构建自主可控的安全体系，实现创新业务可持续的增长。

通过对金融、电商、航旅等业务的深入理解，顶象推出了基于人工智能技术的智能终端、模型平台、风控引擎及关联网络等产品和方案，沉淀了覆盖反欺诈、流量获取、营销获客、平台运营等全场景的行业策略，帮助数千家企业实现了服务的快速落地，助力业务创新与增长，推动企业数字化建设。

顶象总部位于中国北京，在杭州、广州、南京设有分部，先后获得红杉资本、嘉实投资、晨兴资本和东方弘泰资本的数亿元投资。创始人陈树华先生是国内著名安全专家，总裁王天義是原IBM大中华区总经理。公司70%为业务和技术专家，主要来自阿里巴巴、IBM、华为、Capital One、Google等企业，专注于金融风控、人工智能、大数据、安全等领域。

SECTION 01
背景及行业趋势

政策

现状

方案

金融机构面临的挑战

01

政策

2017年5月

中国人民银行成立金融科技（FinTech）委员会，旨在加强金融科技工作的研究规划和统筹协调。强化监管科技（RegTech）应用实践，积极利用大数据、人工智能、云计算等技术丰富金融监管手段，提升跨行业、跨市场交叉性金融风险的甄别、防范和化解能力。

2018年5月

银保监会印发《银行业金融机构数据治理指引》（银保监发〔2018〕22号）引导银行业金融机构加强数据治理，提高数据质量，充分发挥数据价值，提升经营管理水平，全面向高质量发展转变而制定的法规。要求银行业金融机构将数据治理纳入公司治理范畴，并将数据治理情况与公司治理评价和监管评级挂钩，鼓励银行业金融机构开展制度性探索。

2019年8月

中国人民银行印发《金融科技（FinTech）发展规划(2019-2021年）》明确提出，增强金融风险技防能力，正确处理安全与发展的关系，运用金融科技提升跨市场、跨业态、跨区域金融风险的识别、预警和处置能力，加强网络安全风险管控和金融信息保护，做好新技术应用风险防范，坚决守住不发生系统性金融风险的底线。

2019年10月

中国人民银行下发《个人金融信息（数据）保护试行办法（初稿）》，对金融机构与第三方之间征信业务活动等进一步作出明确规定。《办法》第十二条和第十八条规定：“（金融机构）不得从非法从事个人征信业务活动的第三方获取个人金融信息。金融机构不得以“概括授权”的方式取得信息主体对收集、处理、使用和对外提供其个人金融信息的同意。”

现状

随着移动互联网的普及、金融电子化、数字化的进程，高效而灵活的多元化金融服务逐渐渗透到人民群众生活的方方面面。

丰富的金融服务和多样化的应用场景，一方面降低了用户享受便利服务的门槛、极大提升了用户体验；另一方面，速度快、频次高、范围广、场景多等新金融产品的形态，也给金融机构的营销获客、用户体验、风险管理和精细化运营提出了新的挑战。

在欺诈分子横行、从线下到线上对各个场景展开立体化攻击的今天，有着明确分工和缜密“作战”计划的欺诈团伙，娴熟运用各类技术升级欺诈手段，试探和研究目标平台的业务流程和策略，在传统的反欺诈手段无法做到实时而精准的识别、预警与防控的现实情况下，对金融机构的安全展业构成了巨大的威胁。

方案

顶象关联网络是新一代人工智能应用方案，通过充分挖掘金融机构内部的客群特征、业务数据、交易信息、核心征信、合规数据等“数据金山”，基于对金融机构具体业务场景、业务逻辑、产品流程、风险特点的深度理解，科学构建“有内涵、可外延”的复杂关联网络。

再通过应用图数据挖掘、无监督算法、半监督算法、有监督算法等多角度充分挖掘，进而结合应用场景、实际操作人员的具体需求直观而智能的在运营和监测平台呈现最有效信息，从而为多个行业和场景提供反欺诈、精准营销、精细化运营等应用服务，助力业务创新与增长。

- 防控团伙骗贷
- 追溯异常交易
- 定位犯罪洗钱
- 预警养卡套现
- 贷款用途管控

CHALLENGE

金融机构面临的挑战

- 宏观经济形势的动态变化，会影响机构和个人用户的还款意愿、能力和行为。
- 欺诈分子愈加专业，娴熟运用各类技术升级欺诈手段，呈现组织化、团伙化等特点。
- 传统反欺诈手段依赖“非黑即白一刀切”式、评估个体或设备的静态风险行为评分的反欺诈手段，无法在复杂多变的金融业务中，有效防范团伙性的高风险攻击。
- 传统的数据集市，不能完全反映业务的底层逻辑、也不支持高效挖掘关联图谱信息；部分金融机构内部的用户数据、业务数据、交易数据未实现有效打通，无法进行全网的查询监控和全局的评估分析。

SECTION 02
常见团伙欺诈特征

02

组织团伙化

呈现有计划、有预谋的团伙化，团伙内的每个成员接受相关技能的培训，分工明确、合作紧密、协同作案，形成一条完整的产业链。

攻击隐蔽化

对移动互联网、云计算、人工智能各种新技术利用娴熟，欺诈手段日益隐蔽化、取证困难等。

内外勾结化

欺诈分子对信贷业务的申请、受理、调查、评估、审核等的各项流程非常熟悉，通过内外渗透的手段摸清楚金融机构的风控框架和风控规则，专攻业务漏洞。

手段复杂化

团伙欺诈行为更难侦测和识别，依赖“非黑即白一刀切”式、评估个体或设备的静态风险行为评分的传统反欺诈手段，无法从动态的全局视角洞察欺诈风险，无法有效防范团伙性的攻击。

SECTION 03

常见团伙欺诈形式

03

中介包装

熟悉金融机构业务流程的中介机构，通过伪造或包装的证件信息、银行流水、通讯记录、交易记录等，帮助不符合标准的群体申请信贷产品，骗取金融机构资金。

团伙骗贷

虚构生产经营项目、交易、大额商品、抵押物，伪造各类资料，向金融机构申请经营贷款、消费贷款、或抵押贷款，给金融机构直接带来经济损失。

犯罪洗钱

通过金融机构资金账户，进行现金、金融票据、有价证券的财产转换，或者进行转账、结算等方式协助资金转移，掩饰、隐瞒犯罪所得及其收益来源和性质。洗钱不但违法违规，给金融机构带来合规风险，更影响社会金融秩序稳定。

非法套现

信用卡是无抵押、旨在用于消费、提供便利支付的借贷工具。代理机构、不法商户或个人利用技术手段、非法设备等对信用卡等进行大额套现，隐含着较大的逾期和坏账风险。

SECTION 04
关联网络+反团伙欺诈简介

04

反团伙欺诈是关联网络在金融等行业的重要应用，由「关联网络构建」、「关联关系挖掘」和「风险动态监测」三大重要步骤组成

顶象关联网络+反团伙欺诈 能够能够有效防控在申请审批、审批后还款、开户后交易等业务流程中的各类高风险异常行为，为金融机构业务运营和风控人员，提供实时查询、可视化风险监测、风控策略管理、高风险团伙定向分案等服务。从而动态定位潜在欺诈及高风险团伙，从源头追溯作案手段，系统的预测进化趋势，并精准定量评估欺诈等高风险操作的波及范围和影响力度，帮助金融机构快速识别异常操作，高效挖掘机构内外部的潜在欺诈及高风险团伙，增强对未知风险的防范能力，进一步完善和提高金融机构风险管理系统的可靠性和准确率。

- V1.0 主要用于数据的呈现 — 2019.10
- V2.0 实现金融零售场景下的反团伙欺诈 — 2019.03
- V3.0 增加精准营销智能推荐等 — 2019.09

SECTION 05

关联网络+反团伙欺诈的使用步骤

关联网络构建

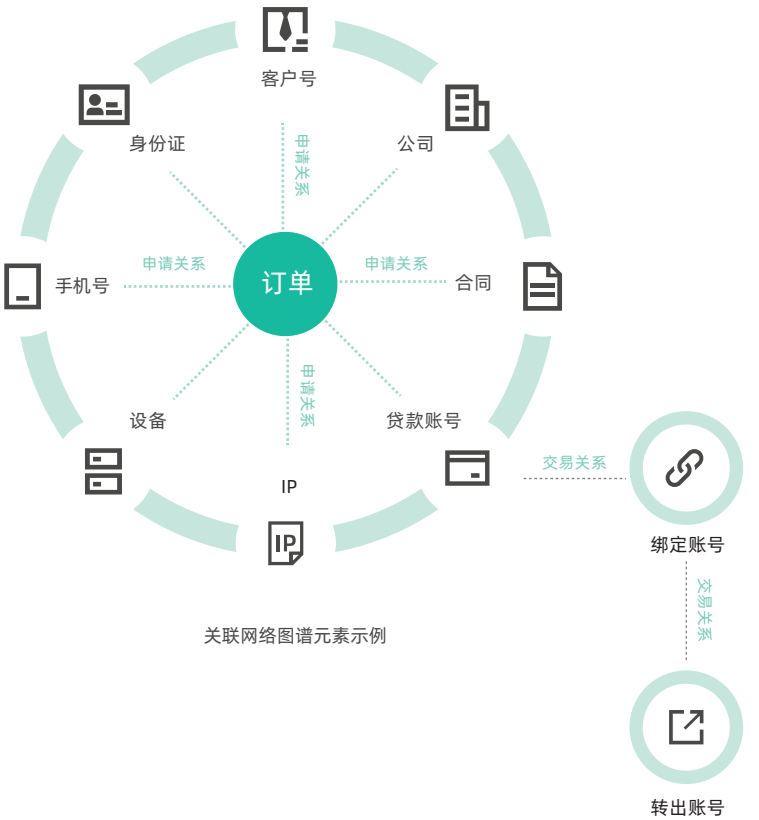
关联关系挖掘

风险动态监测

05

01/ 关联网络构建

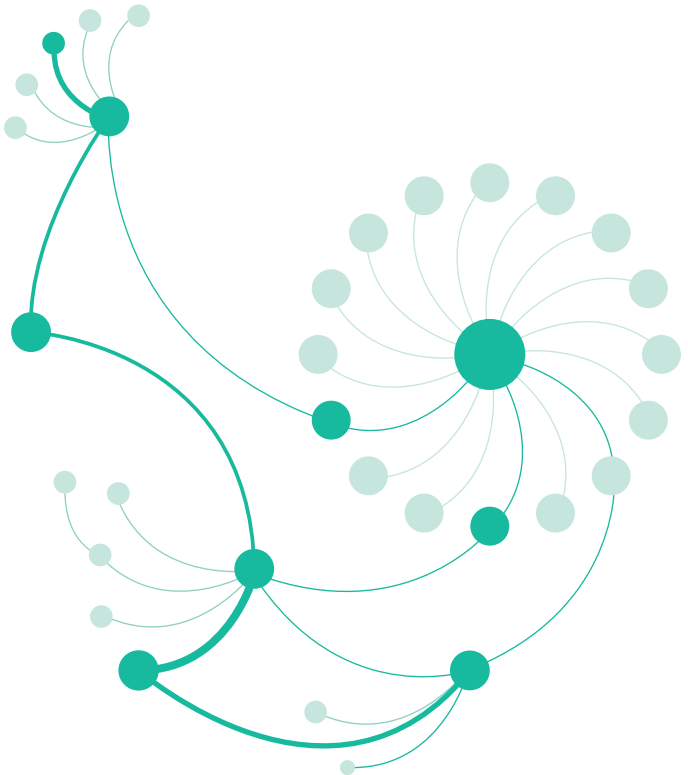
基于对场景需求和业务逻辑的理解，跨部门、跨产品构建覆盖个体、设备、组织、产品、交易等维度的复杂关联网络。



关联网络图谱元素示例

02 关联关系挖掘

提取个体和群体的静态画像、分析动态趋势、通过图数据挖掘技术定位潜在欺诈团伙并进行深度挖掘、特征衍生、应用机器学习定量分析后开发反团伙欺诈模型。



03 风险动态监测

基于反团伙欺诈运营平台的可视化监控台、风控策略管理、黑名单标签库管理、高风险团伙定向分案等服务，有效保障在复杂关联网络反团伙欺诈模型上线后，能够持续更新迭代反欺诈的防控手段、为业务的增长保驾护航。

SECTION 06
反团伙欺诈的应用场景

发现恶意骗贷团伙
挖掘潜在高危团伙
定位高风险贷款中介

06

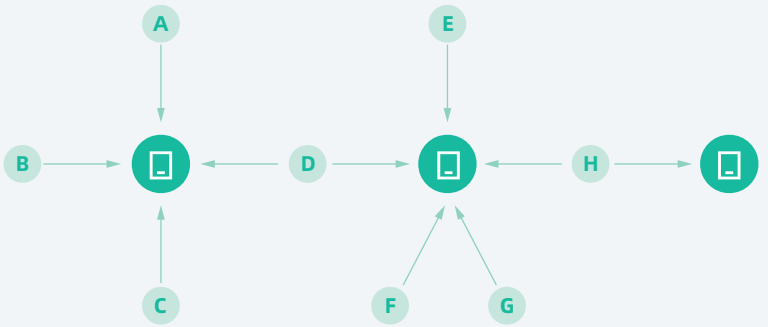
顶象关联网络帮助某金融机构
挖掘出一个15人的骗贷团伙

发现恶意骗贷团伙

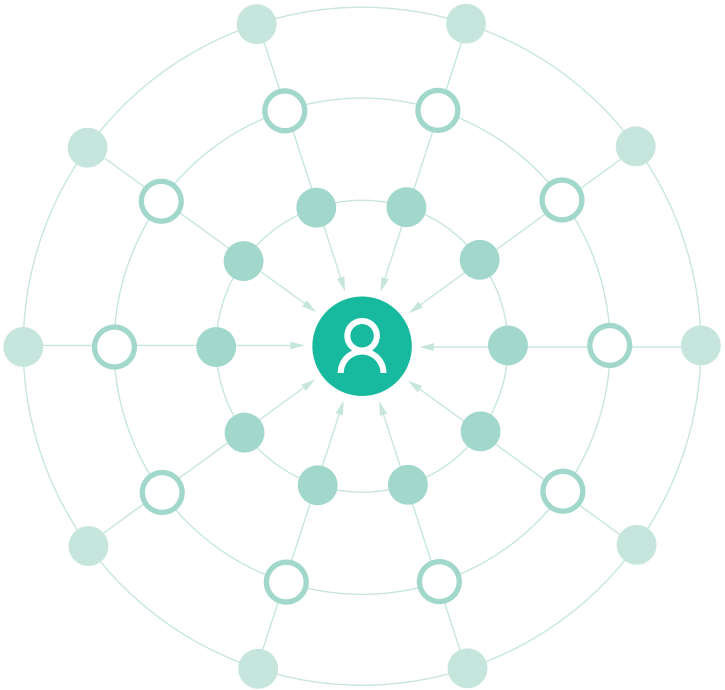
数据显示，在三个月的时间里，15个贷款客户分别提交了15笔贷款申请、三笔通过审批，审批过程中未发现异常。通过关联网络分析发现其中一人与多个设备关联异常，该用户此前多次申请贷款且被拒贷，并且每次拒贷后即更换设备再次发起贷款申请。

进一步的回访和调研确认，这15人是恶意骗贷团伙。通过购买身份证、进行资料包装，反复申请贷款，骗取金融机构资金。

通过进一步的关联追踪显示，该客户先后使用过的、发起贷款申请四台设备在两个月内先后被其他14人使用发起过贷款申请，而使用这些设备申请成功的三笔贷款已经有两笔发生逾期。



挖掘潜在高危团伙



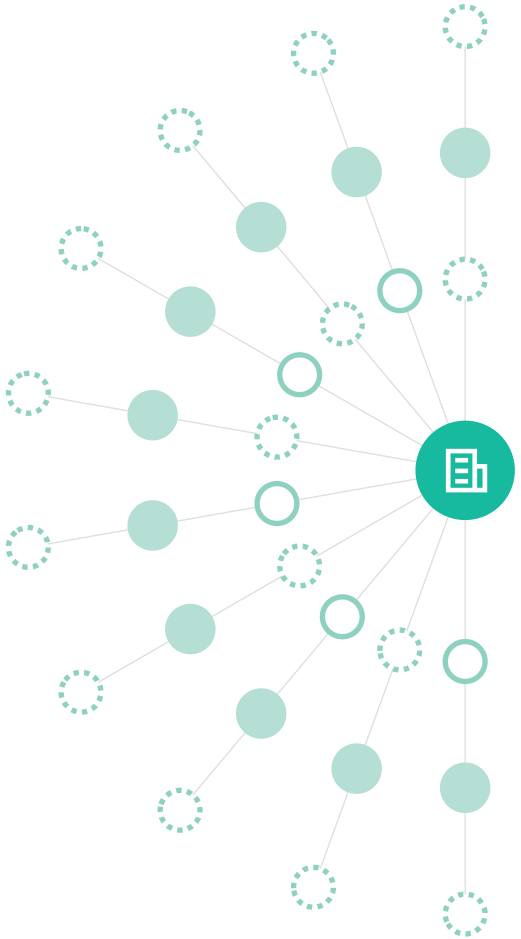
顶象关联网络帮助某金融机构挖掘出
30余名贷款客户组成的异常群体

半年时间内，30余名贷款客户完成贷款申请、审批和放款，每个客户的申请材料真实、审批流程没有异常，符合贷款产品审核要求。

然而，这30余名贷款客户均在申请到贷款后的较短时间内向同一个归集账户转账共50余笔，共转近700万元。进一步的回访和调研确认，归集账户持有人与这30余名贷款账户持有人是同事、朋友、亲戚关系，而贷款的资金被挪用购房。

这30余名申请人如果作为相互独立的、单独的个体来评估，确实信用风险可控。但当大额的借款和偿债压力都归集在同一个人身上时，该客户无力偿还高额贷款的风险是很高的。尤其是经济环境复杂多变，一旦归集账户持有人的还款能力出现问题或资金链断裂，就会出现连锁风险而导致30余笔贷款、近700万元发生逾期甚至违约不良，给金融机构造成的潜在系统性风险和经济损失显著增加，甚至引发系统性风险。

定位高风险贷款中介



顶象关联网络帮助某金融机构识别出多个高风险贷款中介机构及其包装的贷款客户

在半年时间里，130余名贷款客户在贷款成功后，均向某个归集账户发起转账，总转账金额近600万元，每笔转账金额从几千到几万不等，进一步分析发现，转账金额几乎都是其贷款总额的10%左右。经推测和调查确认，这些转账是某贷款中介包装机构收取的服务费，而他们提供的服务，正是根据金融机构的信贷审批规则为借款人包装申请材料。

依靠“量身定做”的包装而获批贷款的客户，本身在信用资质和还款能力上多少存在一些隐患，加上贷款金额尚未到手就被中介机构抽取较高比例的服务费，变相加大融资成本、增加还款压力，最终发生逾期和不良的风险极高。贷款中介包装团伙一旦摸清楚某个金融机构的审批规则，更会短时期内高频包装大量客户进行“批量攻击”，给金融机构带来的挑战和风险极大。

进一步的回访和调研确认，这15人是恶意骗贷团伙。通过购买身份证、进行资料包装，反复申请贷款，骗取金融机构资金。

SECTION 07
反团伙欺诈应用案例

某城商行反团伙欺诈实践
某银行防控信用卡套现实践

07

某城商行反团伙欺诈实践

积极布局发力“数字化”的某城商行， 通过大力推动全行向数字化、智慧化转型，提升零售业务客户服务效率和服务质量。与此同时，也遇到了团伙欺诈风险等诸多新挑战。

顶象关联网络基于该城商行多年积累的海量内部数据，建立了一个自主可控的智能风控系统。能够直观了解网内存在的欺诈团伙、涉案资金，方便审批人员定位与决策；及时而客观的分析存在的欺诈风险、欺诈占比、欺诈团伙来源等，随时掌控全行的风险态势。

同时，帮助该城商行沉淀出四个新的应用成果：

01 客户关系画像体系

基于个贷部、信用卡部、小企业部等多个零售部门积累的申请、交易、贷后等数据，结合产品业务逻辑进行梳理、打通，深度挖掘数据之间的关联关系，构建动态关系网。

02 数据模型平台

可视化模型平台减少业务人员对复杂模型的强编码技能的依赖，在常用的分析和建模场景，平台根据场景应用需求和习惯整合定制化模型包，让具备基本建模能力的人员也可以通过快速培训而具备持续监测、更新和迭代模型的能力。

03 可视化和交互式监控平台

以图关联方式，把团伙直观显示到运营风险平台里面，对疑似欺诈的群体成员进行精准分案，便于业务人员及时排查、开展风险分析以及风险经验的持续打磨和积累。

04 风险监测/预警与防控流程

一方面通过数据驱动型流程将整个风险业务定时参与到业务流程核对中。另一方面，业务打标风险团伙的结果也会沉淀下来，成为模型优化的一个基础。

某银行防控信用卡套现实践

信用卡是最常见金融信贷产品。发卡机构根据申请人的信用资质授予其可以使用的信用额度，申请人可以在多个消费场景使用信用卡额度进行便捷的信用支付，而已经使用的额度可以在还款之后重新恢复、再循环使用于更多的消费支付场景。

“信用卡套现”是指欺诈用户利用不法商户或刷卡设备制造虚假刷卡消费交易，以少量的手续费把信用额度全部转化为个人的现金。常见的套现的方式有“他人消费刷自己的卡”，与商家或某些“贷款公司”、“中介公司”合作套现，或者是利用一些网站或公司的服务等套现。除了信用卡套现，还有欺诈用户进行“以卡养卡”。

借助关联网络，某银行挖掘出数千张存在风险交易的信用卡。对排名一千的高风险信用卡逐一排查发现，其中约80%被确认为套现用户。

关联网络+反团伙欺诈能够有效防控信用卡养卡套现

主要步骤如下：

01

基于申请信息和POS机等交易设备信息，建立信用卡的关联网络

02

计算节点的风险值，并对已知的套现节点进行标注。

03

通过迭代算法，将风险值在网络中进行有效的传播，挖掘出更多潜在信用卡账号。

04

将结果反馈给业务部门，对风险值最大的信用卡账号进行确认。

400-8786-123
www.dingxiang-inc.com
marketing@dingxiang-inc.com