数字金融反欺诈

白皮书

2018年5月31日

京东金融 JD Finance

中国人民大学 金融科技与互联网安全研究中心

中国刑事警察学院 NATIONAL POLICE UNIVERSITY OF CHINA

目录 CONTENTS

序言 1

当前，金融科技的发展及其对传统金融行业的渗透已成为不可逆转的潮流。我们欣喜地看到，金融科技的应用大幅降低了金融领域的信息不对称性，切实推动了普惠金融的发展，为健全多层次金融市场做出极大贡献。然而，事物的发展往往是一体两面的，对于新生事物更是如此。金融科技方兴未艾，但基于此的新型欺诈手段也不断滋生，金融欺诈风险不断升级。

在现阶段守住不发生系统性金融风险底线的宏观背景下，金融监管、防范风险的重要性被提到前所未有的高度。由于数字与金融的"联姻"，金融的欺诈行为呈现出专业化、产业化、隐蔽化、跨区域等新特征，对传统的反欺诈手段形成极大挑战。因此，针对金融领域的反欺诈技术也应不断革新，既要精准打击存在的风险，也要执棋先行，做到防患于未然。

在《数字金融反欺诈白皮书》中，我们有针对性地梳理了欺诈新方式，反欺诈手段，以及在 8 个金融场景中识别、打击欺诈行为的落地实践。这 8 个场景应用涉及网络支付、网络保险、网络借贷、供应链金融、消费金融等领域，既有数字金融的常规业务也有传统金融的创新，既涉及 B 端欺诈也包括 C 端欺诈，既有事前识别拦截也有事后打击制裁，可以说是对数字金融领域的欺诈与反欺诈所做的一次较为全面的总结。

通过白皮书的发布，一方面，我们希望为行业提供一本新型欺诈真实案例的"警示录"，并介绍反欺诈的先进经验；另一方面，我们借此呼吁行业内外的各界同仁携手，共同加强反欺诈技术的研究合作和数据信息共享，为数字金融的碧海蓝天贡献绵薄之力。

数字金融反欺诈是一场持久战，不可能毕其功于一役，只有在技术的不断迭代中实现自身的动态优化，才能取得真正意义上的胜利。反欺诈之路，道阻且长、行则将至！

京东金融研究院院长 孟昭莉

序言 2

数字技术与金融的融合正成为一种不可逆的潮流，金融新模式、新业态不断呈现。然而有光的地方总有影子，技术在创造便利的同时，也带来威胁；金融的巨大外部性可以创造，也可以毁灭。数字金融在发展、升级，伴随技术而来的新型金融欺诈亦是如影随形，各种新手段层出不穷。欺诈事件，一方面不利于数字金融行业的良性发展，另一方面也对传统金融的创新业务造成了诸多不利的影响。严峻形势之下，反欺诈刻不容缓。

反欺诈是金融行业永恒的主题，在《数字金融反欺诈白皮书》中，我们从数字金融欺诈的特点和传统反欺诈手段的不足出发，具体阐述了数字金融反欺诈的主要技术手段在具体情境中的应用。新型金融欺诈步步紧逼下，传统的反欺诈手段无所适从，解决问题的手段必须是与时俱进的，技术是决定数字金融反欺诈取得实效的关键。白皮书中的 8 个典型的反欺诈场景应用，详细阐述了欺诈手法，重点介绍了反欺诈技术。数据的采集、分析、以及最后据此做出的决策在每个反欺诈案例中都落到了实处。这以一种更加直观的方式呈现了问题以及问题的解决之道。

无序且不受监管的个人数据使用是欺诈产业得以"壮大"的重要基础，数据的安全问题显得尤为重要。同时，数字金融欺诈多样化、产业化、隐蔽化、场景化的特点，决定了反欺诈方式必须从孤军奋战走向联合打击。此外，反欺诈不仅仅是针对既已发生的诈骗行为，事前做好防止工作，防患于未然、打击于无形才是上上之选。

如《双城记》中所言："这是最好的时代，也是最坏的时代。"一方面，技术在发展，数字金融不断自我革新；另一方面，层出不穷的数字金融欺诈避之不及，只能直面。放眼金融科技的未来，我们怀着希望，也要保持警惕。《数字金融反欺诈白皮书》仅仅是开始，希望它能够起到抛砖引玉之效，激发各方对此的关注、思考，为促进数字金融行业的健康发展、维护数字金融行业的秩序贡献绵薄之力！

中国人民大学金融科技与互联网安全研究中心主任 杨东

序言 3

技术的革新下，金融的新模式、新业态不断涌现，对公共安全和社会治理也提出了诸多新问题，如何有效管控这些新模式、新业态，使其朝着正确的轨道稳步前进，是摆在行业和监管部门面前的共同难题。近年来，数字金融行业呈现出涵盖广、多元化、增长迅速的特点。与此同时，也有部分欺诈者利用技术、监管和公众意识等方面的不完善，演绎着千变万化、层出不穷的欺诈行为。令人欣慰的是，这也在一定程度上刺激了反欺诈技术的升级、改造和优化，更促使监管部门更多关注数字金融行业的合规发展。

《数字金融反欺诈白皮书》首先总结了数字金融欺诈的主要特点，在此基础上梳理了反欺诈技术的详细分类，然后基于选取的 8 个金融场景，认真分析每一场景下惯用的欺诈手法、反欺诈的先进技术以及反欺诈效果的可移植性，力求深入简出、剥丝抽茧地解析反欺诈技术如何精准识别打击欺诈行为的复杂过程。特别值得一提的是，为使读者更清晰快速地了解每个案例，本报告采用形象直观的可视化图形，真实还原了看似繁琐的欺诈手法，勾勒出反欺诈技术进行打击的逻辑路线图。

从数字金融反欺诈的实践经验来看，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。其中，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。“路漫漫其修远兮，吾将上下而求索”。只有立净化行业之志，举全行业之力，在反欺诈体系建立上加强合作、信息共享、共防共御，良性健康的数字金融生态圈才能逐步形成。

中国刑事警察学院网络犯罪侦查系主任 秦玉海

核心观点

◎ 数字技术与金融行业融合发展，催生数字金融新业态。与此同时，金融欺诈风险不断扩大，反欺诈形势严峻。

◎ 数字金融欺诈呈现出专业化、产业化、隐蔽化、场景化四大特征。

◎ 传统反欺诈手段维度单一、效率低下、范围受限，难以应对新型的欺诈手段。

◎ 数字金融反欺诈技术主要包括数据采集、数据分析、决策引擎三大类型，结合运用能够解决传统反欺诈技术面临的诸多问题。

◎ 在网络支付、网购运费险、网络借贷、供应链金融、网络营销、消费金融、手机银行、农业保险等八大领域，数字金融反欺诈技术已经得到广泛应用并取得良好效果，具备向其他领域进一步移植、复制的可能。

◎ 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。其中，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。

1 金融欺诈风险不断升级

- 数字技术与金融行业融合发展，衍生出涵盖第三方支付、网络保险、网络借贷、供应链金融、消费金融、传统金融创新业务等数字金融的新模式、新业态。
- 数字金融欺诈风险不断升级，网络黑产发展肆虐，影响了消费者对数字化金融服务的信任程度。
- 异常平台和平台漏洞数量持续攀升，数字金融领域反欺诈形势严峻。

数字技术应用于金融，极大地解决了金融领域中信息不对称的问题，但新型的欺诈形式和手段也不断衍生。无论是根植于数字技术的金融业务还是传统金融的数字化，欺诈事件都层出不穷。这一方面不利于数字金融行业的良性发展，另一方面也为传统金融的数字创新业务带来诸多消极影响。

一、数字技术与金融结合催生新业态

在“互联网 +”的大趋势下，数字技术与金融不断交融。国内金融科技创业公司、创新业务模式与解决方案不断涌现，涵盖第三方支付、网络保险、网络借贷、供应链金融、消费金融、传统银行创新业务等领域（见图 1）。一方面，新兴的数字金融机构不断渗透到传统金融业务中，另一方面，传统机构也多方介入数字金融。

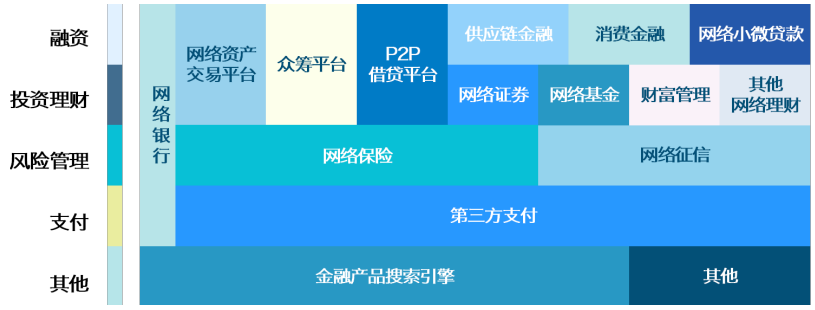

图 1　互联网环境下，金融新业态

二、数字金融欺诈风险不断升级

数字技术的支撑下，金融市场的体量和发展潜力被逐步放大。与此同时，其暴露的风险隐患也与日俱增，欺诈现象层出不穷。从数字金融平台欺诈的角度看，违约欺诈平台占比已超六成。以网贷平台为例，截至 2017 年年末，累计问题平台数量为 4039 家，占网贷平台总数的 67.7%[1]。从个人欺诈的角度看，由网络黑产主导的数字金融欺诈发展肆虐，已经渗透到数字金融营销、注册、借贷、支付等各个环节。据统计，2017 年黑产从业人员超 150 万，年产值达千亿级别，应用数据分析手段开展金融业务的数字金融平台是黑产攻击的主要对象之一[2]。

从市场的客观反映来看，数字金融的风控环节普遍面临较大压力。根据国家互联网金融安全技术

专家委员会数据显示，截至 2018 年 4 月，其互联网金融风险分析技术平台发现了 21624 个存在异常的互联网金融网站和 1362 个互联网金融网站漏洞（见图 2）。

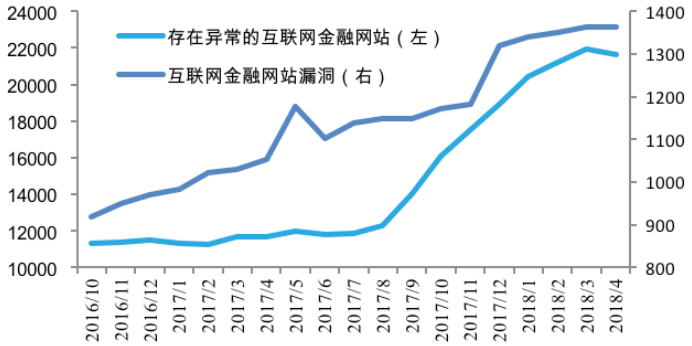

图 2　存在异常的互联网金融网站和网站漏洞（单位：个）

数据来源：国家互联网金融安全技术专家委员会

从消费者的主观认知来看，欺诈高发降低了中国消费者对数字化金融服务的信任程度。信息服务公司益博睿与数据调研机构 IDC 联合发布的亚太地区《2017 年欺诈管理洞见》，基于数字化接受水平、行业偏好、欺诈率，以及对企业欺诈管理能力四个变量制定了"数字化信任度指数"。调查发现，满分 10 分的前提下，中国对数字化金融服务的信任得分仅为 3.87 分，低于亚太平均水平（见图 3）。

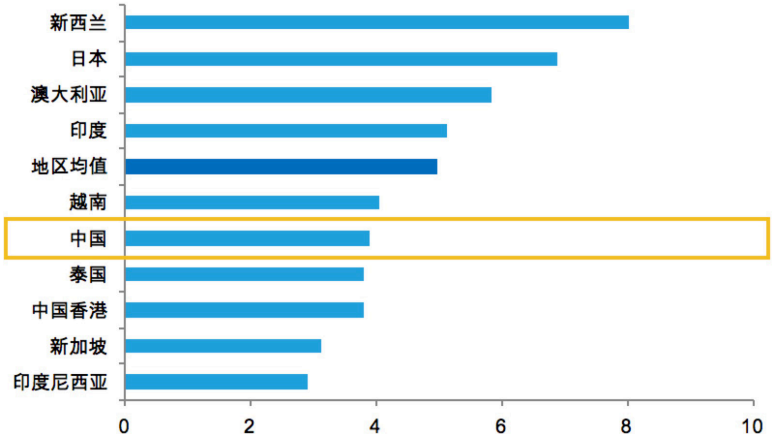

图 3　亚太地区数字金融信任化水平

数据来源：《2017 年欺诈管理洞见》

1　比达咨询 (BDR) 数据中心，《2017 年度中国 P2P 市场研究报告》

2　电商安全生态联盟发布的《电子商务生态安全白皮书》

2 金融反欺诈手段不断演进

- 数字金融欺诈手段表现出专业化、产业化、隐蔽化、场景化的特征。
- 专业化即欺诈方向更加精准、手段更加多样；产业化即欺诈分子往往有组织、成规模、分工明确、合作紧密、协同作案，形成一条完整的犯罪产业链；隐蔽化即欺诈行为更加隐蔽，主要表现为异地作案、小额多发、取证困难；场景化即由于多数数字金融业务依托特定的场景开展，相应的数字金融欺诈也呈现出场景化特征。
- 传统的金融反欺诈技术面临新的欺诈形式暴露出诸多不足，包括维度单一、效率低下、范围受限等。
- 数字金融反欺诈技术能够解决传统反欺诈技术面临的诸多问题，从技术的运用层级和着力点划分，主要包括数据采集、数据分析、决策引擎等三大类型。

根植于数字技术的金融业务快速发展，加之传统金融行业不断向线上转移，由此引发的金融欺诈形式不断更新、纷繁复杂，相应的欺诈手段呈现出专业化、产业化、隐蔽化、场景化的特征，传统反欺诈手段在新形势下面临诸多挑战。通过数字金融反欺诈技术不断的自我革新，能够解决传统反欺诈技术所面临的维度单一、效率低下、范围受限等难题。

一、数字金融欺诈的主要特点

数字金融欺诈逐渐表现出专业化、产业化、隐蔽化、场景化的特征。

（一）欺诈专业化

数字金融欺诈手段由之前较为简单的盗号、盗刷演变为现在的借助大数据等前沿技术，从撒网式向精准化转变，并叠加传销、兼职赚钱、网购退款、金融理财、虚拟货币等更为复杂多样的手法（见图 4）。多样的诈骗手段加之数字金融、区块链等新词汇的注入使得数字金融诈骗更具迷惑性，不易被识别，受害人防不胜防。

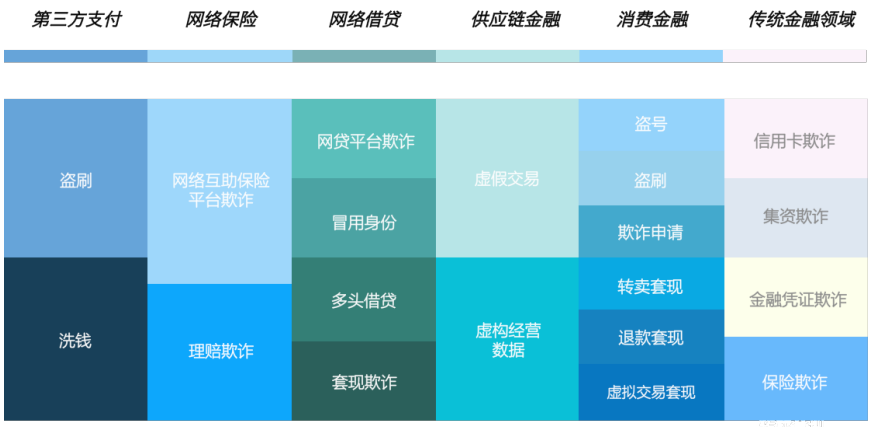

图 4　不同领域数字金融欺诈行为列举

（二）欺诈产业化

同传统的诈骗相比，数字金融诈骗往往是有组织，成规模的，他们分工明确、合作紧密、协同作案，形成一条完整的犯罪产业链。这条产业链主要包括开发制作、批发零售、诈骗实施、洗钱销赃四大

环节，进而又细分为软件开发、硬件制作、网络黑客、钓鱼零售、域名贩子、个信批发、银行卡贩子、电话卡贩子、身份证贩子、电话诈骗、短信群发、在线推广、现金取现、电商平台购物、黄赌毒网站等 15 个具体分工（见图 5）。

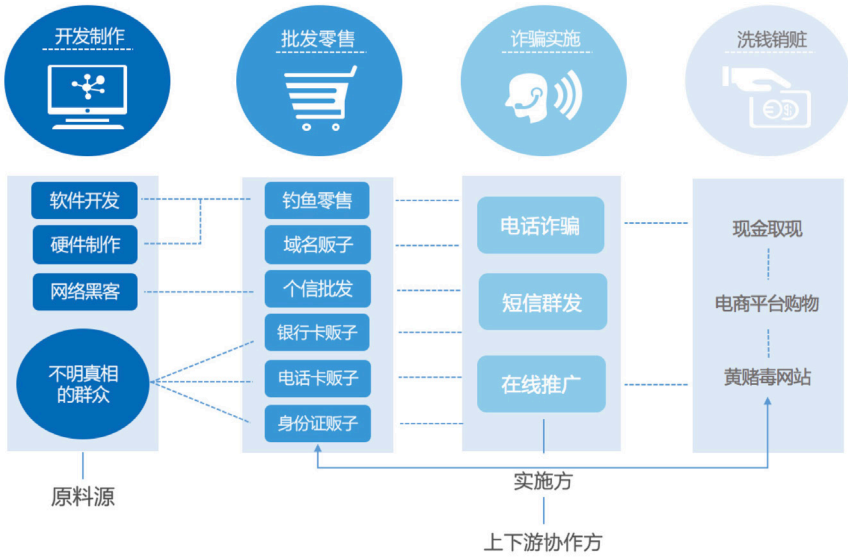

图 5　数字金融诈骗基本链条

（三）欺诈隐蔽化

互联网等技术的虚拟特性导致欺诈更为隐蔽，主要体现在三个方面：一是异地作案，金融欺诈逐渐呈现出移动化趋势，数字金融诈骗不受空间限制，甚至同一诈骗团伙的犯罪分子都来自全国各地；二是小额多发，由于数字金融具有普惠性，服务客户下沉，单笔诈骗造成的损失多数都在万元以下；三是取证困难，数字金融诈骗多存在盗号盗刷、冒用身份问题，仅仅依靠传统手段很难取证。

（四）欺诈场景化

多数数字金融业务依托特定的场景开展，相应的金融欺诈也呈现出场景化特征。以网购场景为例，数字金融机构依托网购这一场景可以开展消费金融、供应链金融、退运险等多种金融业务，如果买卖双方勾结，虚构交易行为，则可能出现同一场景下的多种欺诈行为。商户卖家客户获得虚增交易量，获取供应链金融更高额度的授信，买家可能通过虚假购买行为，利用消费金融套现，此外，双方还能通过退货骗取运费险赔付。

二、传统反欺诈技术面临的挑战

维度单一、效率低下、范围受限是传统反欺诈技术面临的三大挑战。

（一）维度单一，央行征信系统覆盖率不足

传统反欺诈手段维度单一，很难对用户形成多维度的用户画像，进而通过用户画像对客户的行为偏好、偿债能力、支付能力和欺诈倾向做出分析。以央行征信为例，由于数据来源单一，我国尚有 4 亿信用白户（没有过信用卡和其他借贷记录），降低欺诈风险需要构建多维度的征信体系。

（二）效率低下，难以服务日益下沉的客户群体

传统反欺诈技术需要大量人工操作，应用成本高，效率低下。金融科技业务客群下沉，交易频繁、实时性强、数据量大，欺诈呈现出小额、高频的特点，传统反欺诈手段很难服务逐渐下沉的客群。

（三）范围受限，难以应对日益场景化的诈骗行为

随着数字技术的深入发展，金融欺诈和其他场景的结合日益紧密，呈现出“跨界”的特点。如网络购物、网络游戏等非金融场景中也蕴含金融欺诈风险，这些风险利用传统反欺诈技术很难识别。

三、数字金融反欺诈的主要技术手段

在欺诈团伙产业化、规模化，且广泛使用大数据、人工智能等前沿技术的今天，反欺诈技术能力直接影响着数字金融反欺诈的实际效果。从技术的运用层级和着力点来看，数字金融反欺诈技术可分为数据采集、数据分析、决策引擎等类型。

数据采集

数据采集技术主要是应用于从客户端或网络获取客户相关数据的技术方法。值得强调的是，数据采集技术的使用，应当严格遵循法律法规和监管要求，在获取用户授权的情况下对用户数据进行采集。数据采集技术包括：设备指纹、网络爬虫、生物识别、地理位置识别、活体检测等等。

数据分析

数据分析技术是指运用数据分析工具从数据中发现知识的分析方法。其中，机器学习技术是一种通过模型预测来反欺诈的数据分析技术。机器学习技术依赖数据，通过对数据的整理分析训练出合适的模型，再利用模型进行预测，达到反欺诈的效果。它包括有监督机器学习模式、无监督机器学习模式和半监督机器学习模式。

决策引擎

反欺诈决策引擎是数字反欺诈体系的大脑和核心。一个功能强大的决策引擎，可以将信誉库、专家规则和反欺诈模型等各类反欺诈方法有效的整合，并为反欺诈人员提供一个操作高效、功能丰富的人机交互界面，大幅降低反欺诈运营成本和响应速度。对于决策引擎好坏的判断，应当从引擎处理能力、响应速度、UI 界面等多个维度进行综合判断。

3 数字反欺诈在不同金融场景中的应用

本章在对数字金融欺诈不同领域表现形式进行概括的基础上，选择了八个典型的欺诈场景，针对各个场景中的欺诈手法，重点介绍了反欺诈技术及其应用的真实案例，并分析了技术应用的可移植性。

本章八个欺诈场景

- 场景 1　网络支付

在网络支付环节，诈骗分子通过社工和技术手段，盗取用户账户，进行盗刷、洗钱等行为。行为序列、生物探针和关系图谱技术可做到前中后期对欺诈行为预警。行为序列记录用户购买历史，生物探针研判用户手机使用习惯，关系图谱则从人际关系网络对用户进行信用估算，三者结合形成立体人物画像，在反欺诈、盗刷以及群体涉黑挖掘场景中均可发挥作用。

- 场景 2　网购运费险

虚构交易骗取保费是网购运费险欺诈的常用手法，利用大数据和机器学习技术能够在事前对保险产品进行差异化定价，在事后预测欺诈的概率。此外，这些技术也能移植到账户险、车险、医疗险等领域的欺诈行为识别中。

- 场景 3　网络借贷

身份冒用是网络借贷中常用的欺诈行为，利用人脸识别、用户画像技术能够刻画客户个人的特征，并用于网络贷款交易事前、事中、事后全过程的欺诈识别。这两类技术不仅在网络借贷虚假申请识别中的应用效果显著，同时也可复制到传统银行业务的信用申请环节。

- 场景 4　网络营销

利用虚假号码注册后批量扫货下单是营销优惠欺诈中的常用手法。首先利用黑名单技术筛选疑似羊毛党的用户，若命中黑名单则直接拦截。在此基础上，利用设备指纹识别技术和机器学习模型能够有效阻击利用设备进行营销欺诈的羊毛党。设备指纹技术在对用户行为的追踪分析和征信数据获取方面具有很大的应用价值。

- 场景 5　供应链金融

供应链金融欺诈归根到底就是将虚假的企业经营数据，作为供应链授信的依据。利用机器学习、关系图谱和设备指纹识别等技术，能够关联出企业在供应链上的经营关系，从而判断企业真实的经营状况。这几类技术的综合运用解决了需要大量人力物力进行信用主体身份核实和资料验真的问题，不仅仅在供应链金融，在消费金融、传统银行业务等领域均可高效使用。

- 场景 6　消费金融

在消费金融领域，诈骗分子骗取身份信息，在分期购物平台或现金贷平台套现，应用设备指纹、生物探针、行为序列等技术手段可以在事前防范、事中识别、事后拦截套现欺诈行为，该反欺诈技术手段可以在套现、盗刷等领域推广、应用。

- 场景 7　手机银行

在手机银行领域，诈骗分子利用木马病毒控制受害人手机，盗取其手机银行钱款。应用生物探针技术可以实现用户的身份判定，识别欺诈分子的恶意登陆行为并实时拦截。这项技术可向"手机防盗"等非金融领域移植应用。

- 场景 8　生猪保险

在生猪保险领域，投保欺诈和重复骗保行为严重侵蚀保险公司利润，应用 "猪脸识别"和区块链技术能够为每头猪建立"唯一可识别编码"，并实现信息互通互享，自动识别保险欺诈和重复报案行为，该技术可向宠物保险领域移植应用。

场景 1 网络支付

我国网络支付发展迅速，从 2013 年始，网络支付市场的交易规模平均以 50% 的年均增速增长。2017 年，我国网络支付交易规模达到近 154.9 万亿元，同比增长率接近 44.3%。网络支付在线下小额和零售领域等适用场景不断丰富，渗透于消费、金融、个人应用等各个领域。

新的支付形式也催生了新的欺诈手段。在支付环节，黑色产业集团往往通过社工方式和技术手段，盗取利用个人姓名、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，并进一步用于进行精准诈骗、恶意营销。虚假 WiFi、病毒二维码、盗版 APP 客户端以及木马链接等是盗取用户私人信息的主要手段，获得的关键信息被收入数据库分类储存，其中，账户信息（如游戏账户、金融账户）通过黑色产业链进行金融犯罪和变现，用户真实信息除了贩卖外，更多用于商城盗刷。

网络支付欺诈案例：盗用账号支付

某大学生发现自己银行卡里的 5 万元“不翼而飞”。反复查询，他被通知自己在某电商平台注册了一个新账号，购买了高达 49966 元商品。实质上并非本人的购买行为。其实，该商城风控部门利用其风控体系在支付的那一刻已触发预警。接到预警后，风控负责人快速安排对这一订单的拦截，同时安排发货以进一步锁定嫌疑人，最终帮助挽回损失。

该案例是账号盗用的典例，其涉及四步具体操作（见图 6）。

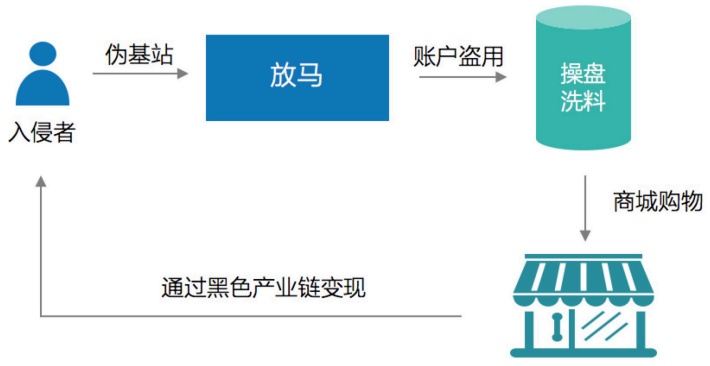

图 6 盗用账号支付 - 欺诈过程

第一步：放马。该团伙在大学城周边，通过伪基站发送带有木马病毒链接的伪装短信，该学生在点击链接后，用户名及密码均已泄露；第二步：操盘。由于直接盗刷银行卡难度较高、风险较大，骗子掌握各类信息之后，便想起通过商城购物的方式来进行变现。第三步：洗料。注册完账户，绑定银行卡之后，就会通过网上商城购买高价值物品，比如黄金、手机等。并通过对来电进行拦截或者设置呼叫转移，使得商品到达欺诈团伙手中。第四步：变现。通过地下黑色产业链销赃网络，将购买来的物品变现、分赃。

反欺诈手段

该案例中，主要运用了行为序列、生物探针和关系图谱技术对支付环节的前中后期进行了风险预判（见图 7）。

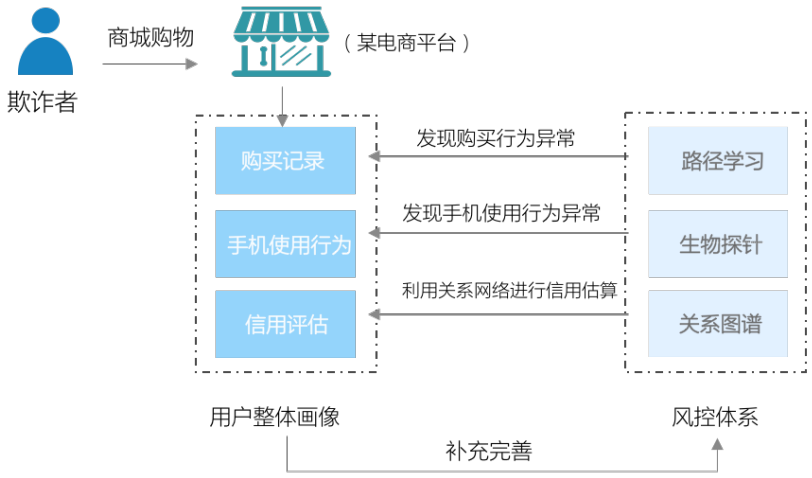

图 7　盗用账号支付 - 反欺诈过程

首先，行为序列技术发现了购买记录的异常。行为序列技术记录了该学生在平日购物时的购物金额、浏览时长、对比行为等因素，发现了购物金额不超过 1000 多元、平时要花时间进行同类对比、寻找优惠券的该学生，本次仅浏览了十分钟便下单购买昂贵的商品，马上触发了预警。其次，生物探针技术发现本次购买行为与往常不同。生物探针技术能够根据用户使用 APP 的按压力度、手指触面、滑屏速度等 120 多个指标，判断用户的使用习惯，因此，检测出本次购物中的异常使用情况。最后，关系图谱技术，通过用户关系估算用户的信用，同时周围与之相关人的信用影响到对该用户信用评估。关系图谱技术通过分析发现该学生对本商品的需求并不高，因此也触发了预警。

反欺诈效果和可移植性

行为序列、生物探针、关系图谱等技术综合运用，可以有效识别支付环节的用户风险，同时可向其他场景复制、移植。

行为序列技术对用户购物行为、地址位置信息、过往订单信息、信用卡交易详情等信息进行实时监测，形成多维度用户画像。除了应用于用户身份识别和反欺诈，行为序列分析还能实现"千人千面"的精准营销。根据用户的历史购买和浏览习惯等信息可以推测出用户的年龄、性别、职业、爱好等身份特征，比如某位用户经常浏览母婴网站并购买孕期用品，则可推测该用户为一位准妈妈，进而可根据这些信息在不同时间为用户推荐恰当的商品，提高购买率。

生物探针技术打破了传统判别用户身份的逻辑，基于用户的行为特征模型，而不是仅仅依靠密码、验证码这些易被盗用的数字信息识别用户，这种技术应用在金融场景中效果尤其明显，但同时也可向其他非金融领域复制、移植。一是可以将生物探针这一技术手段广泛应用于社交、游戏、购物等各类移动 APP 账户安全保护中。智能手机及各类账户中存储着用户的大量信息，包括朋友联系方式、照片、数字资产甚至工作机密资料，一旦手机丢失或账户被盗，后果难以估量。目前应用的账户安全保护技术主要为数字密码、手势密码、手机验证码等数字信息，容易被不法分子攻击、破解，若加入生物探针技术，将能够从更多的维度判别用户身份，且不存在被盗风险。二是生物探针技术可以同账户安全险、手机丢失险等网络保险产品结合，帮助保险公司完善产品结构。生物探针技术集合上百项指标生成特有的用户行为特征模型，可有效进行人机识别和本人识别。若应用于账户安全险、手机丢失险的产品设计中，可有效降低出险率，同时帮助用户进行安全管理，让保险产品不仅能管理风险，还能保障安全。

关系图谱技术可以进行涉黑群体挖掘。通过记录用户节点信息，以及所有在这些节点上发生行为的相关行为的连接，最终把与之相关的一系列用户和行为都描述出来。它能有效识别数据造假、组团欺诈、辅助信贷审核、失联企业管理等等。在这个维度上做风控，可以将隐蔽在后面的欺诈行为提前预防、并拦截在体系之外。除了能识别金融领域的欺诈风险之外，关系图谱技术还可对持股结构、高管关系、涉诉案件等方面的欺诈行为有效识别。关系图谱技术的主要特点是能够勾勒出看似不相关的主体间的隐含关系，从而对潜在风险的识别非常有效，从这一点上讲，关系图谱技术非常契合金融业务尤其是数字金融业务参与主体多、流程冗长的特点，能够在复杂的业务流程中梳理出一条简单清晰的主线，这不仅能够识别欺诈行为，而且对于某个业务场景下全局性金融风险的识别防范具有非常现实的意义。

场景 2 网购运费险

中国保险行业协会数据显示，截至 2017 年上半年，互联网保险保费收入较 2012 年实现了 20 余倍的增长，特别是运费险、账户险等轻型险种呈现快速发展的趋势，并使许多碎片化、个性化、场景化的保险需求得到满足。以运费险为例，某电商平台推出运费险后退货纠纷率由 2.15% 下降到 2.12%，客服介入概率降低了 50%。与此同时，由于互联网保险险种的多样化，以及线上平台投保的便利性，滋生出了很多新型骗保的欺诈行为。同样以运费险为例，某公司上市运费险之初的赔付率竟高达 90%，骗保的比重可想而知。因此，如何利用反欺诈技术构建科学有效的风险识别监控体系，已成为互联网保险行业亟需解决的问题。

无论是传统保险还是互联网保险，保险欺诈的主要类型主要有先出险再投保、隐瞒危险、虚构保险标的、重复投保，这些欺诈行为的根本目的是为了骗取保险金，只是在欺诈手段上略有差异。以运费险为例，其欺诈包括四个步骤：首先在网络购物平台注册店铺并购买快递单号；然后进行虚假发货，同时购买运费险；第三步，购买快递单号进行虚假退货；最后，在虚构收到退货的事实后骗取运费险（见图 8）。

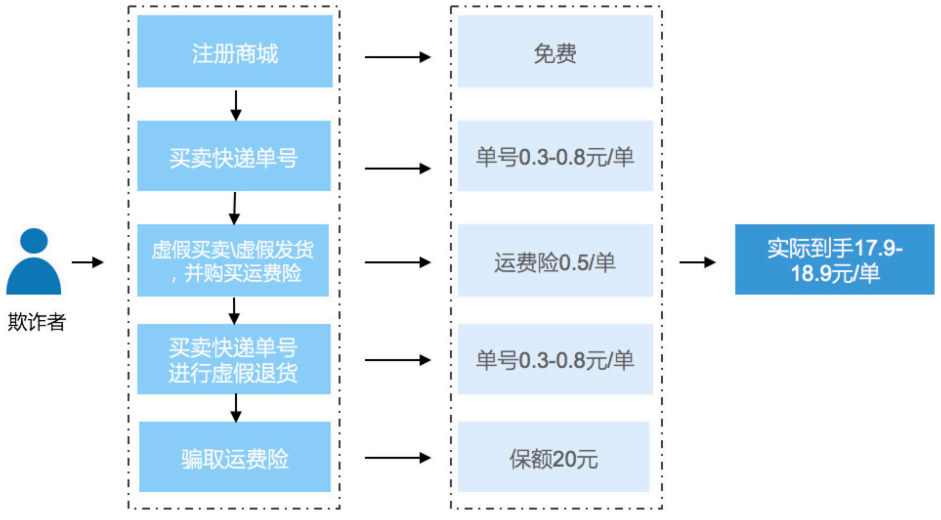

图 8 网购运费险 - 欺诈过程

运费险欺诈案例：利用虚假交易骗取运费险

2017 年 9 月，某保险公司营业部向警方报案称，有人利用在某网络商城的店铺进行虚假交易，骗取保险公司退赔的运费险。保险公司发现，去年 7 月这三家店铺的交易量突然暴增，2000 多个买家集中下单，生成 7.5 万多笔订单，且这些订单最终都是退货并退赔运费。退赔运费每单 20 元，4 个月的时间，保险公司为这三家店铺退赔了 200 多万元。

反欺诈手段

运费险反欺诈主要运用了大数据分析技术和机器学习技术，反欺诈的重点集中在事前定价和事后出险两个阶段（见图 9）。

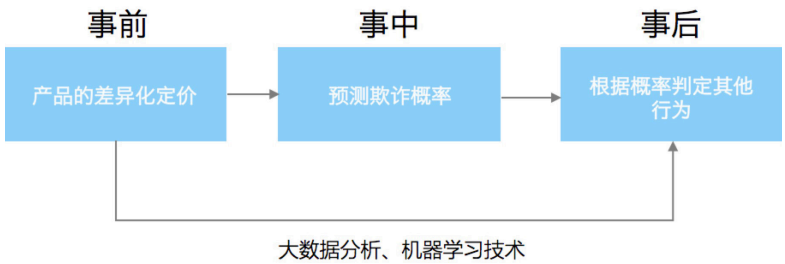

图 9　网购运费险 - 反欺诈过程

利用大数据和机器学习技术实现运费险产品的差别定价。从客户、商家及产品的多个维度分析，建立机器学习模型，通过模型预测出险的概率，结合产品定价方法对运费险保费实现精准计算，进而实现针对不同投保人的差异化定价。运费险差异化定价主要有三个特点：首先，进行风险定价的数据更加精细。保费和保额将利用买家、卖家在电商平台上的每一笔交易进行精准定价。其次，运费险中进行风险定价的数据更加全面。运费险定价中不仅依照投保人在其公司的内部数据，还可利用电商平台、快递公司提供的用户所有数据，甚至可获得同业公司的相关数据。这些数据极大丰富了风险刻画的维度，使得定价更加全面准确。最后，运费险中进行风险定价的数据是实时的。利用信息技术实时跟踪个体买家或卖家的情况，风险数据可以实时更新，定价也随着风险因子的改变而改变。

利用大数据和机器学习技术识别理赔欺诈。运用大数据及机器学习算法，预测案件在不同环节发生欺诈的概率，根据预测结果将案件分划分为不同等级，制定差异化处理方案。

反欺诈效果和可移植性

利用大数据、机器学习等人工智能技术，极大提高了互联网保险的数据获取途径、获取量以及对数据的掌握程度，给保险定价和理赔提供了详细信息。2017 年某电商平台利用反欺诈技术避免的运费险损失就高达 2000 万元。此外，这些技术也能移植到账户险、车险、医疗险等领域的欺诈行为识别中。

从大数据分析的应用趋势来看，不仅在数字金融，在医疗、教育、交通、体育、政府管理等各个行业都能得到广泛应用。大数据分析技术应用的部分共性问题需要引起注意：一是规范数据标准，提高数据可用程度。大数据分析涉及的数据庞杂、混乱，数据的整合难度较大，在数据整合中容易出现结果偏差；二是大数据分析需要海量的数据基础，需要行业内甚至跨行业的数据共享；三是加强敏感信息保护，防范信息泄露风险。

机器学习技术通过计算机手段实现模拟或学习人类的行为，是人工智能的核心技术，可广泛应用于保险、反洗钱等金融领域及物流、医疗等非金融领域。以在反洗钱中的应用为例，反洗钱监控不仅要监测账户的交易行为，还要在相对较长的时间段对个交易行为进行模式分析，应用人工智能技术能不断学习不法分子的洗钱套路并有效识别、精准打击。

场景 3 网络借贷

我国网络借贷行业出现早、发展快。自 2007 年，我国第一家网络借贷平台拍拍贷成立。经过数年的发展，我国 P2P 网贷规模已经成为世界第一。据网贷之家的数据显示，2017 年全年网贷成交量接近 2.8 万亿元，相比 2016 年增长 0.8 万亿元，接近 2015 年成交量的 3 倍。

网络借贷行业快速发展的同时欺诈行为也层出不穷，据爱钱进网的统计，每 100 个拒贷案件中大约有 16 起涉及不同程度的蓄意造假或欺骗。由于线上造假成本低廉，诈骗技术不断更新，代办公司迅速崛起，社会个人征信体系不完善等原因，网贷行业也成为诈骗者竞相追逐的"蛋糕"。

网络借贷的欺诈行为主要有中介代办、团伙作案、机器行为、账户盗用、身份冒用和串联交易等。其中，身份冒用是比较常见的欺诈行为，它是指贷款人对提供的个人身份、财产证明等材料进行造假，甚至采用欺骗等违法手段获取他人信息，进而冒充他人身份骗贷。

网络借贷欺诈案例：网络借贷中的身份冒用欺诈

2017 年 3 月，某中介通过 QQ 群招揽学生做兼职，中介给予每个学生一张手机卡，并要求学生拿此卡去银行办理工资卡。中介以登记为由，利用银行卡和手机号获取了学生的身份证、学籍、学历等信息，而后用绑卡方式向网贷平台申请了多笔信贷业务（见图 10）。

图 10　网络借贷 - 欺诈过程

反欺诈手段

针对身份冒用的欺诈行为，主要采取了人脸识别、用户画像等技术。

具体步骤包括：一方面，利用人脸识别技术识别是否是借款人本人发起的申请，具体操作上利用视频画面截取申请人脸部特征，与身份证照片进行比对验证。但由于该网贷平台没有视频验证的流程，就需要配合精准画像等技术进一步验证；另一方面，通过文本语义分析、用户行为分析、终端分析等等方法，刻画客户个人的特征，并用于网络贷款交易事前、事中、事后全过程的欺诈识别。例如，通过大数据分析投资者的行为轨迹发现，正常投资者会在申请的每个节点都停留几秒，完成整个贷款申请流程至少需要 5 分钟，而数据分析发现欺诈者不到 10 秒钟就走完所有流程，，且该用户的申请时间是凌晨 2 点。根据对用户申请速度、申请时间的分析，就可以判定出来这个人应该是欺诈者，于是平台立即拒绝了其贷款申请（见图 11）。

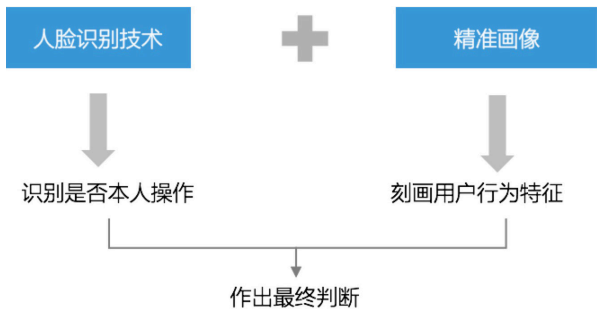

图 11　网络借贷 - 反欺诈过程

反欺诈效果和可移植性

人脸识别和用户画像技术在身份冒用的欺诈行为识别中发挥了重要作用，通过图像采集、人脸检测、精确定位、数据标准化、人脸特征比对等步骤识别是否是本人操作，利用用户画像能够锁定客户的个性化特征，综合判定欺诈的可能性。这两类技术不仅在网络借贷虚假申请识别中的应用效果显著，同时也可向其他金融及非金融领域移植，复制。

人脸识别技术除在金融反欺诈中得到应用外，还可在公安刑侦、社会保障、边境检查等公共服务领域得到广泛应用。当然，该技术也存在一定的风险：一是脸部数据的可复制性，个人的脸部特征数据可在公开环境下直接获取并复制。二是脸部数据的不稳定性。脸部化妆、过敏、受伤、整容都

会导致脸部特征发生变化，从而影响人脸识别准确率甚至无法识别。三是后台数据的安全性至关重要，一旦人脸识别、虹膜识别的后台数据被黑客攻破，对行业和社会都是毁灭性的打击。因此，人脸识别技术并不是风控中具有绝对杀伤力的武器，而应该结合反欺诈的其他技术手段配套使用，这是人脸识别技术运用的重要前提。

用户画像技术的本质是给用户行为贴标签，该技术的主要作用是通过数据挖掘，利用关联规则计算以及聚类算法分析用户偏好行为以及行为之间的内在联系。因此，该技术不仅能够识别用户潜在的欺诈行为，更重要的是能准确了解用户习惯和需求，在基于用户需求角度下的各类商业场景和公共服务场景都有应用的可能。值得注意的是，用户画像技术是多学科的结合，需要知识图谱、自然语言处理、机器学习和数据挖掘等方面的交叉融合。

场景 4 网购营销

营销欺诈即俗称的“羊毛党”，是指有选择地参与各互联网渠道的优惠促销活动，以相对较低的成本甚至零成本换取物质上实惠的人群。界定羊毛党的关键特征是，多频率、有组织地在单次营销活动中多次获取优惠金额的行为，其实质是由于其薅羊毛的行为侵占了其他用户本应享受的优惠活动，这种行为即是打击的对象。目前，羊毛党已形成 15 余工种、160 余万从业人员、产业规模不低于 1000 亿元人民币的产业链，分工明确、合作流程成熟，并且逐渐向隐蔽、专业、精准方向发展。以某上市公司力推直播软件的营销活动为例，为获取客户量，只要注册软件就能获得奖励金并立即提现。2016 年底，该公司投入近 16 亿元后净亏损约 10 亿元，最终被 ST，而其中大部分奖励被羊毛党撸走，这说明羊毛党的行为已经严重影响了企业的正常经营。

羊毛党的主要类型：第一类是个人纯手工进行薅羊毛的行为，这类行为往往因涉案金额和规模小，不易受到商家的重视；第二类利用商家网站或 APP，使用外挂程序将薅羊毛过程完全自动化；第三类通过破解后台接口建立虚假客户端进行薅羊毛；第四类是团伙羊毛党，通常是组织者利用 QQ 群、微信群指挥团伙成员薅羊毛，且这类薅羊毛行为呈现与平台、商家瓜分利益的趋势。

羊毛党的欺诈步骤为：首先，利用虚假号码进行批量注册，有些还会配合模拟器或 IP 地址修改工具进行；其次，利用上述账号进行集中的批量扫货下单；最后，将买到的明显低于市场价格的商品，以比较合理的价格倒手卖出，赚取差价（见图 12）。

羊毛党欺诈案例：营销优惠欺诈

某网上商城每周六推出满 80 减 20 活动，活动开始后一个月发现大量订单支付失败，其中金额恰为 80 元的订单占比较高，且这些订单绑定的支付卡余额均为 60 元。该商城风控部门利用其风控体系及时识别了疑似薅羊毛的订单，并在支付时进行事中拦截。

反欺诈手段

在识别羊毛党的过程中，主要使用了设备指纹识别技术和神经网络模型等机器学习技术。

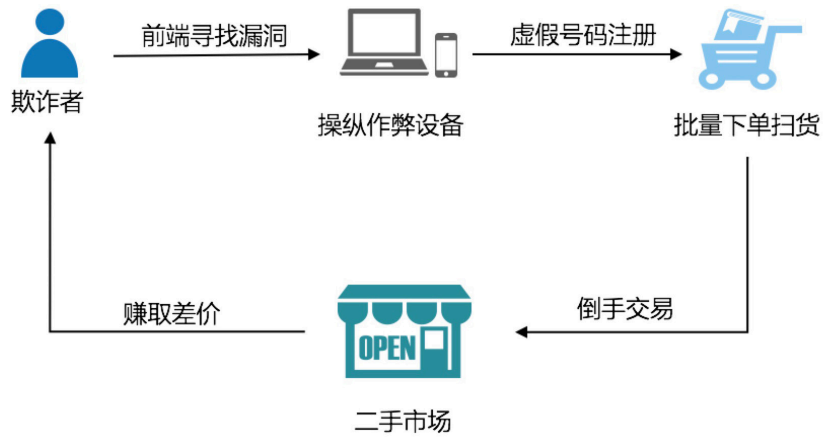

图 12　网络营销优惠 - 欺诈过程

具体步骤包括：首先，利用黑名单技术筛选疑似羊毛党的用户，若命中黑名单则直接拦截。在此基础上，综合运用设备指纹技术和机器学习技术识别羊毛党的欺诈行为。一是利用设备指纹技术识别出部分羊毛党在一台终端设备上登录上千个 PIN 码进行操作，同时发现出现大量金额恰好为 80 元的订单，据此判断存在欺诈的可能。二是利用机器学习技术对用户的购物行为、交易习惯、交易次数等数据进行综合分析后，判断该用户是否为羊毛党（见图 13）。

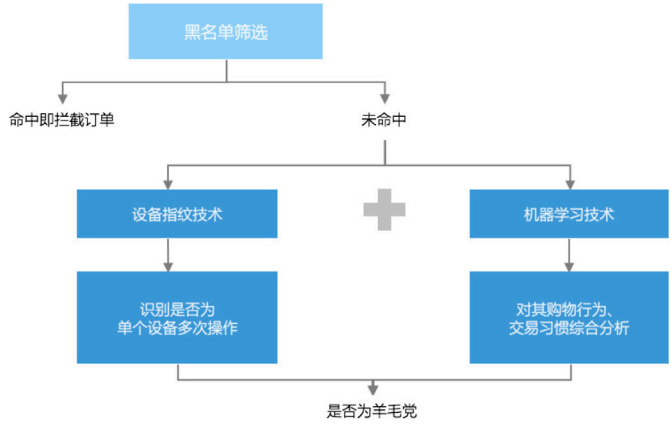

图 13　网络营销优惠 - 反欺诈过程

反欺诈效果和可移植性

该案例最终拦截近 10% 的支付订单，为商家挽回 100 余万元的损失。据估算，采用反欺诈技术

每年能为全行业节约 10%-50% 的营销优惠成本。设备指纹识别技术配合机器学习模型能够有效阻击利用设备进行营销欺诈的羊毛党。

设备指纹识别技术根据不同的识别方法，大体上可分为主动式、被动式和混合式三种。三种方式在隐私保护、响应速度和准确率方面存在一定差异。设备指纹识别技术在数字金融领域的应用集中体现在两个方面：一是对用户行为的追踪和分析，比如购物网站会采集用户的设备信息，并根据设备指纹信息对用户进行相关的商品推荐，实现精准营销。更为重要的是，利用采集的信息形成设备指纹，给用户提供更好的安全保障，比如检测到用户的风险登录、更换设备登录要求用户进行二次验证等等；另一方面，利用设备指纹技术记录用户在互联网上的活动并进行信用评分，这将对互联网征信体系健全起到极大的促进作用。

机器学习技术的可移植性参考场景 1。

场景 5 供应链金融

供应链金融是指金融机构将核心企业和上下游企业联系在一起提供灵活运用的金融产品和服务的一种融资模式，它在为中小企业拓宽融资渠道、为银行等金融机构开源新财路等方面效果显著。2014 年以来，受益于应收账款、商业票据及融资租赁市场的不断发展，供应链金融在我国发展较为迅速。一方面，供应链金融正不断创新求变，探索新模式、新市场、新领域，在解决中小企业融资难方面发挥了重要作用，推动了商业生态的发展；另一方面，由于参与主体众多、欺诈风险难以识别和控制，也制约了行业长期健康发展。

供应链金融企业欺诈行为的本质是利用经营数据造假来骗取供应链信贷支持的行为，因此，供应链金融欺诈归根到底就是企业经营行为的欺诈，具体表现在采购收回扣、销售截留货款、财务挪用公款、营销套取渠道费用、招投标索贿、售后虚报维修费用、生产虚构加班费、行政虚报管理费等等。这些欺诈行为一旦被认定为真实的经营数据，并以此作为授信依据，将对供应链金融发展产生巨大的风险隐患（见图 14）。

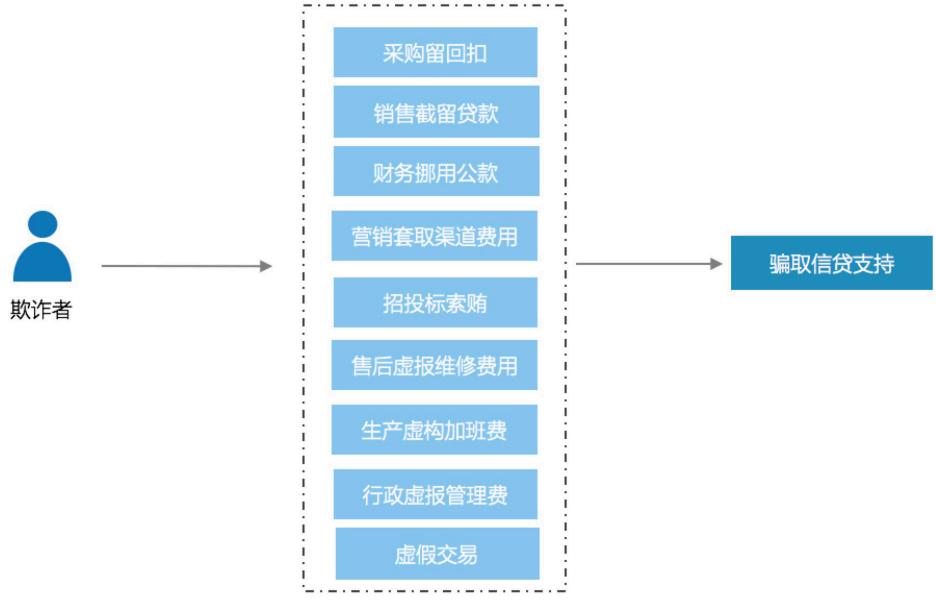

图 14　供应链金融 - 欺诈过程

供应链金融中企业欺诈的案例：企业经营数据异常的欺诈

某上市公司 A 企业接受尽职调查时提供给会计师事务所和券商的财务报表，除了银行贷款是真实的，隐瞒了应收账款、销售利润、民间借款、对外担保等信息存在造假的事实。而此时，B 企业作为 A 企业的关联公司，向某线上平台提出了贷款申请（但 B 企业并没有告知平台其为 A 企业关联公司的关键信息）。

反欺诈手段

在识别上述企业的经营欺诈行为时，主要利用了机器学习、关系图谱和设备指纹识别等技术。具体步骤包括：第一步，运用机器学习等技术对 A 企业的公开信息进行自动化审计后发现，其企业经营数据不真实。第二步，在发现 A 企业存在经营欺诈行为后，该线上平台自有的企业图谱及舆情系统利用公开的上市公司报告信息，能够描绘出包括注册地址、股东结构、经营范围、组织形态等信息在内的数千家企业关系图谱，关联出 B 企业是 A 企业的关联公司；第三步，由于 B 企业对线上平台提出了信贷申请，因此需要利用机器学习技术对 B 企业的经营数据等信息进行全方位审核。与此同时，利用设备指纹技术和机器学习技术发现 B 企业存在刷单欺诈行为（具体技术细节见场景 4 中营销欺诈案例）。第四步，综合 B 企业与 A 企业的关联关系事实和 B 企业刷单炒信的行为，该线上平台拒绝了 B 企业的信贷申请（见图 15）。

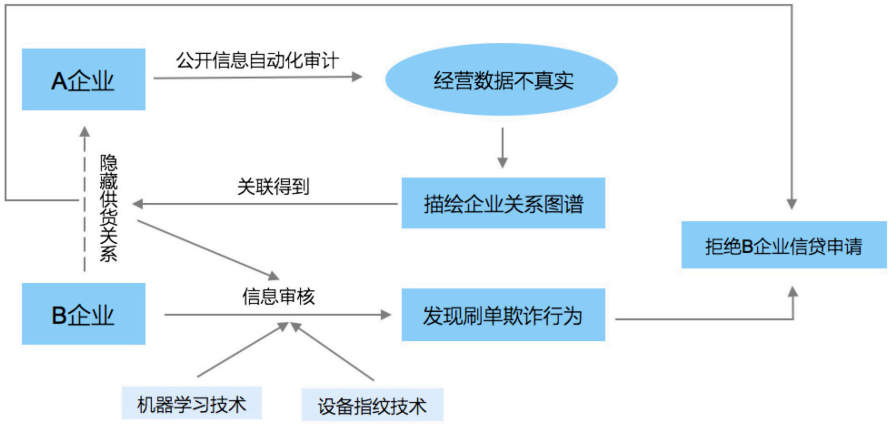

图 15　供应链金融 - 反欺诈过程

反欺诈效果和可移植性

企业隐瞒经营信息并骗取信贷支持的行为，是供应链金融中比较常见的欺诈现象。综合运用设备指纹识别技术、关系图谱和机器学习技术，解决了需要大量人力物力进行信用主体身份核实和资料验真的问题，特别是关系图谱技术能够将企业经营行为表现在图上，从而呈现出不同企业的关联性和聚集性，增强识别企业欺诈行为的能力，能够极大地提高了此类欺诈行为的精准打击率。

各技术的可移植性参考其他场景。其中，关系图谱参考场景 1、机器学习参考场景 2、设备指纹参考场景 4。

场景 6 消费金融

消费金融行业发展不断规范，前景依然广阔。艾瑞咨询数据显示，2017 年，中国消费金融市场交易规模近 2 万亿，相较 2016 年增长 128%。从资产端看，消费金融市场分为消费分期和现金贷两类，其中消费分期覆盖网购、租房、汽车、旅游、装修、教育、医美等行业和场景。

随着行业不断发展，专门从事消费金融欺诈的黑色产业也愈加猖獗，不法分子盯上了各类分期购物平台和现金贷平台，想方设法让其成为实施诈骗转账汇款的"工具"。监测数据显示，超过 40% 的逾期订单发生在疑似诈骗的用户群中，一旦黑客通过违法冒用客户信息申请到贷款，这笔订单注定违约。

消费金融的诈骗套现行为可能发生在账户注册、激活、登陆、交易、信息修改等各个环节。一是犯罪分子可能盗用空白身份信息，自己注册消费金融平台账号进而完成一系列的套现操作；二是用户本身注册过消费金融平台账号，不法分子通过拖库撞库等手段盗取账号，冒名登陆套现诈骗；三是受害人在不知情的情况下，陷入犯罪分子编织的骗局，客观帮助犯罪分子完成整个诈骗过程。最常见的冒用身份诈骗一般分两步进行，首先骗取身份信息或账号信息，不法分子利用网络、短信等发送假网站、假链接骗取账号密码，验证码，或冒充中介、客服直接骗取客户信息；然后冒用身份在消费金融平台进行借贷或购物套现。

消费金融欺诈案例：冒充中介，以兼职为名骗贷套现

某电商平台后台系统检测到某范围内的几个移动终端在短时间内通过多个账号登录平台，分期购买手机等数码产品，且购买习惯也同以往不同。发现这一情况后，平台及时拦截其继续交易并报案。

警方经侦查发现，包括黄某、王某等三人组成的犯罪团伙在附近的几所高校，谎称中介"借取"学生账号信息进行"刷单"并支付商品价值 10% 的费用，同时向学生承诺不需要学生承担任何还款义务和风险。实际上三人冒用这些身份信息在分期网站上购买手机等数码产品，准备销售套现后跑路。由于网站报案及时，警方及时为大学生挽回损失并将犯罪分子绳之以法（见图 16）。

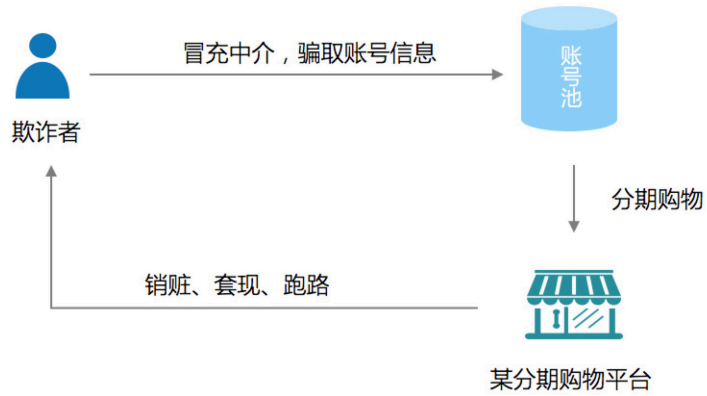

图 16　消费金融 - 套现欺诈过程

反欺诈手段

设备指纹、生物探针、行为序列技术在事前、事中、事后全流程反欺诈

在反消费信贷套现欺诈过程中，主要应用了设备指纹、生物探针、行为序列等多项先进智能技术。设备指纹技术通过用户指纹为每个用户账户建立唯一的 ID，一旦发现冒用身份登录行为，可及时拦截；生物探针技术通过采集用户在使用设备的按压力度、设备仰角、手指触面等使用习惯，为其建立专属的行为模型，发现异常操作及时阻止；行为序列技术可以将用户的购买行为同历史购买习惯进行比对，预警可能发生的欺诈行为。 在上述的案例中，诈骗分子通过移动终端在短时间内登录多个账号申请消费分期产品，且专门挑选价值较高、易变现的数码产品进行购买这一异常行为，触发了电商平台的反欺诈预警。

上述反欺诈手段，不仅可应用在事后，还可对账号的异常登录和交易行为进行实时、多维度、动态校验，在事前、事中防范、识别欺诈风险（见图 17）。

事前评估　依托大数据技术建立完善的风控模型和应用策略体系，能够剔除高风险用户，为安全交易建立第一道防线，防患于未然。

事中监控　风险订单监控系统可以对异常账户和套现风险进行实时监控和全面预警。通过各类数据接口、技术手段和安全体系对异常交易进行拦截。

事后处理　将识别出的套现欺诈信息关联扩散后加入黑名单体系，进行策略和模型优化升级，从而更精准的识别和拦截欺诈交易，提高欺诈分子的作案成本。

图 17　消费金融 - 反套现欺诈过程

反欺诈效果及可移植性

设备指纹、生物探针、行为序列等反欺诈技术手段可广泛应用于借贷类互金业务及各类账户安全反欺诈中，有效监测异常的注册、交易、登陆行为，降低欺诈风险，同时该类技术手段还可向信用审核领域复制移植。

综合运用各技术手段可实现全线上、零人工的授信和放款，相比于传统手段，信贷审核效率提高 10 倍以上，客单成本降低 70% 以上。传统的线下信贷审核需要依赖人工实地调查，获取客户授权打印征信报告，调取银行资金流水，担保人担保等繁琐流程。利用技术手段分析客户的账户基本信息、资金流信息、交易信息、物流信息等可从更多维度形成客户的精准画像，进而为不同客户匹配不同的授信额度。值得注意的是，实现线上信审必须依托线上交易场景并沉淀足够的历史数据信息。

各技术的可移植性参考其他场景。其中，生物探针和行为序列参考场景 1、设备指纹参考场景 5。

场景 7 手机银行

商业银行对金融科技的发展日益重视，逐步加大在技术建设方面的投入。各银行纷纷利用互联网技术和手段，拓展包括直销银行、网上银行、手机银行等多元化的服务渠道，提升用户体验，增加用户粘性。随着智能手机的广泛普及应用，手机银行已成为商业银行的客户服务主要渠道之一，《2017 年中国银行业服务报告》显示，我国手机银行个人客户已达 15.02 亿，同比增长 57.52%。

在电子化渠道深化创新下，相应的欺诈手段与反欺诈技术也不断进化。根据中国银行业协会《中国银行业产业发展蓝皮书》数据，2016 年中国信用卡欺诈损失排名前三的欺诈类型分别为伪卡、虚假身份和互联网欺诈。诈骗电话、钓鱼网站、木马病毒、短信劫持是诈骗分子的惯用伎俩和套路。随着人们防备的增加，诈骗分子的手法也越来越精准，他们会根据不同的人群特征，精心编造出各种主题实施诈骗，如会议邀请、包裹藏毒等。

手机银行欺诈案例：会议邀请二维码植入木马病毒

某公司员工打开手机邮箱，发现一封主题为会议邀请的邮件。打开会议邀请，提示可通过扫描邮件二维码注册信息，该员工对会议主题很感兴趣就用手机扫描了二维码并填写相关信息报名参会，几天后，发现自己网银账户中的两万元钱被盗。

事实上，会议邀请完全是骗子编造的钓鱼邮件，而二维码被植入木马病毒，该恶意控制应用会偷偷申请手机权限，隐藏图标，进而控制受害者手机，手机里的敏感信息进而被回传到骗子的邮箱，骗子通过后台登录受害者的网银账户，将钱款转移（见图 18）。

反欺诈手段

生物探针技术判别用户身份

生物探针技术，可以在用户操作手机 APP 时采集到包括手指触面、线性加速度、触点间隔等数百个行为指标，根据历史行为数据，通过机器学习计算专属行为模型，在用户操作手机时，可以将其

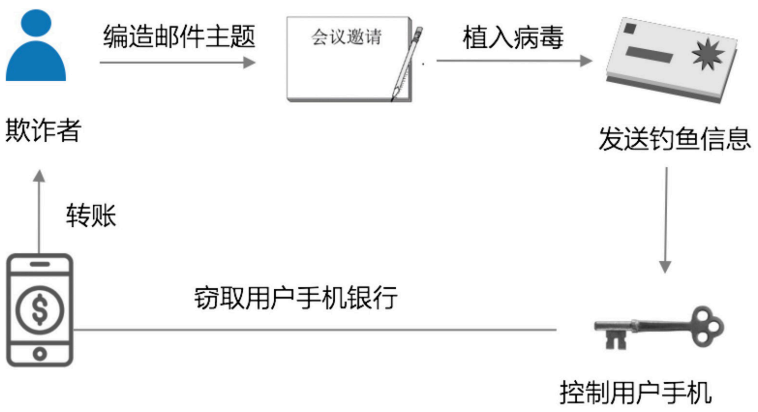

图 18　手机银行 - 欺诈过程

当前操作习惯同历史模型比对，判断这个人是否为风险用户，实现用户的身份判定。这项技术应用于反欺诈和防盗刷的场景中，将能减少甚至避免风险事件的发生。在上面提到的案例中，如果应用了生物探针技术，将能够及时识别欺诈分子的恶意登录行为，并阻止转账行为的发生（见图 19）。

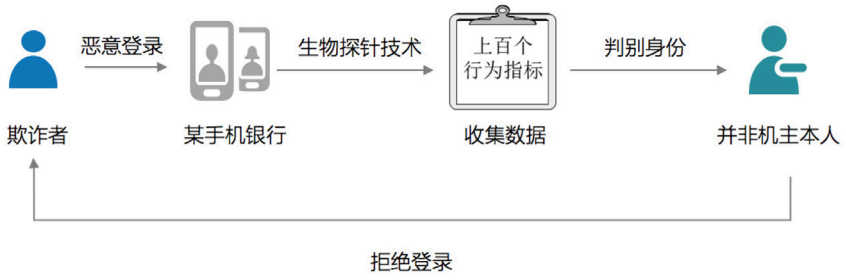

图 19　手机银行 - 反欺诈过程

反欺诈效果和可移植性

生物探针技术打破了传统判别用户身份的逻辑。基于用户的行为特征模型，而不是仅仅依靠密码、验证码这些易被盗用的数字信息识别用户，这种应用在金融场景中效果尤其明显，但同时也可向其他非金融领域复制、移植。生物探针技术的可移植性参考场景 1。

场景 8 生猪保险

农业保险在乡村振兴中发挥着重要作用，但我国农业保险目前还主要依靠国家财政转移支付，商业保险占比较低。2004 年原保监会正式启动政策性农业保险试点，至 2017 年我国农业保险已经覆盖全国所有省份，实现保费收入 479.06 亿元，支付赔款 334.49 亿元，参保农户 2.13 亿户次，受益农户 5388.3 万户次。但由于保费收费低、经营成本高、操作难度大、出险率高等原因，我国商业农险发展举步维艰，发生在农业保险领域的理赔欺诈，让本就发展受阻的农业保险处境更加艰难。

生猪保险是农业保险的重要险种之一，由于理赔欺诈及出险成本过高等原因，一直处于亏损状态。生猪保险的理赔欺诈主要有两种类型，一是投保欺诈，比如一个农户共养了 100 头猪，但只给其中的 50 头猪投保，100 头猪中任何一头猪出现死亡都会向保险公司索赔，由于保险公司很难识别出险的猪是否投保，赔付率倍增；二是重复骗保，即猪死亡后，养殖户串通保险公司勘察员对死猪反复拍照，谎报死猪数量重复骗保。

生猪保险欺诈案例：保险公司勘察员串通养殖户骗保

某保险公司勘察员小张在半年时间内，多次串通养猪户投保人虚报保单、并自导自演死猪假现场，骗得保险理赔款 15 万元。后案件告破经警方问讯，原来，小吴半年前为某养殖户办理理赔勘察时，养殖户为了多获得保费，悄悄塞给小吴一包香烟并请他“通融”一下，后来两人合谋对死猪从不同角度拍照骗取保费。小吴发现这一“商机”之后又多次“指导”其他养殖户骗保，并从中收取好处费（见图 20）。

反欺诈手段

猪脸识别、区块链技术，解决“活体唯一识别问题”。

上述生猪保险理赔欺诈的主要问题在于运用传统手段，很难解决“活体唯一识别问题”，将“猪脸识别”和区块链技术结合运用，可有效解决这一难题。一是“猪脸识别”采用迁移学习算法，可从不同角度进行猪脸信息采集，自动识猪，可以为每一头猪建立“唯一可识别编码”；二是由于从“小猪”到“大猪”的

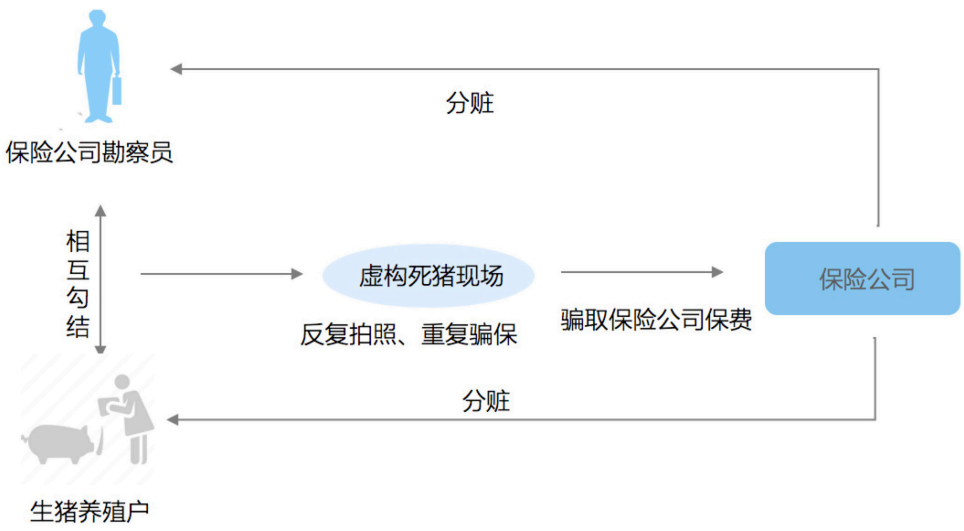

图 20　生猪保险 - 欺诈过程

全养殖周期中，猪的外貌特征会发生较大变化，可选择若干关键节点，在猪的外貌特征没有发生质变的时刻不断更新图像数据，确保"唯一可识别编码"的连续性；三是运用区块链技术建立反欺诈信息共享平台，将投保信息以及历史索偿信息上链存储，有新的赔付事件发生时，只需将照片信息上传就能自动识别保险欺诈和重复报案行为（见图 21）。

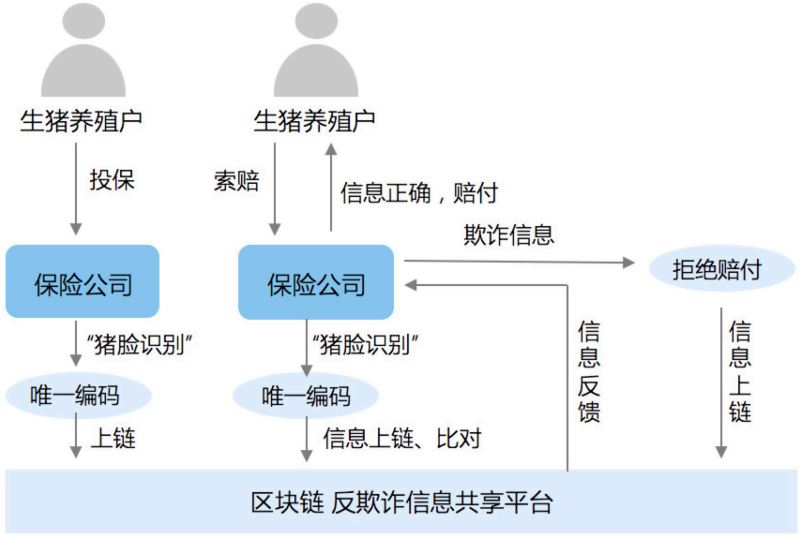

图 21　生猪保险 - 反欺诈过程

反欺诈效果和可移植性

运用"猪脸识别"和区块链技术可有效防止理赔欺诈，增加保险公司的盈利能力，从而促进农业保险持续、健康发展。

以"猪脸识别"为代表的图片识别技术还可向以下两个领域复制、移植。

一是应用在死猪无害化处理理赔产业链上，降低理赔成本。根据国务院要求，在 2020 年前要完成死猪无害化处理体系建设。原来养猪户发现死猪后，需上报保险公司，保险公司派勘察员现场勘察，确认之后等无害化处理厂将死猪回收处理后，保险公司才能进行理赔，整个流程耗时费力。应用"猪脸识别"技术，可以将整个流程线上化，养殖户只需将死猪照片上传给保险公司和无害化处理厂，无害化处理厂将猪回收，处理前在传送带再对死猪进行拍照匹配，便可实现自动化理赔，每头猪的理赔成本由原来的 6 元钱降低为 6 毛钱，节省 90% 的理赔成本。

二是优化 "单体"养殖管理流程，降本增效。在农业养殖过程中，需要对一些价值较高的单体单独建档管理，以对"种猪"的管理为例，猪场需要对每头种猪建立数据档案并每天更新数据信息，传统流程包括棚舍信息采集、纸笔记录、EXCEL 录入、系统录入等多个环节，耗费大量的人力、物力。应用"猪脸识别"技术可在养殖技术人员巡查猪舍时，直接对猪进行拍照识别，并将相应的信息录入到智能手机应用中，后台自动对每头猪的档案信息进行跟踪记录。值得注意的是，在实际落地应用过程中，由于环境遮挡、光线、移动等问题，会影响识别精准度，针对这一问题，可将"猪脸识别"和二维码识别技术结合运用，用产品方案弥补技术落地中遇到的实际问题，为行业提供更便利、可行的解决方案。

区块链技术的分布式存储、去中心化、不可篡改等特征，决定了其除了应用在金融反欺诈领域之外，还能改善众多金融及非金融场景的流程效率、降本增效。在资产证券化、资产托管、医疗、教育、政务等领域，区块链技术正在广泛应用。

4 建议和展望

- 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。
- 数据获得是反欺诈体系建立的根本前提，强化对数据使用的安全保护、扩大央行征信系统的征信范围和加强信息披露，是反欺诈体系发展完善的当务之急。
- 中性的技术决定了其既可以被不法分子利用行诈骗之事，也可以服务于匡扶正义的反欺诈事业。一方面，我们要不断优化反欺诈模型和系统构建，综合运用多种技术手段对欺诈行为进行精准打击；另一方面，要将先进的技术在行业内共享，优秀企业的技术输出值得鼓励。
- 要从根本上弱化欺诈的动力源，需要我们不断优化机制。首先，要提高金融科技企业的门槛，做到扶优限劣。其次，需要多方共同合作，构建由监管部门、行业协会、金融机构、科技企业共同参与的反欺诈联盟。

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。其中，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，这三者的关系是相辅相成、相互促进。未来数字金融反欺诈之路应该从数据、技术和机制三个方面均衡发力：

数据是基础

数据获得是反欺诈体系建立的根本前提，获取征信主体在时间、空间等多维度的数据记录，是对其进行有效信用评估不可或缺的条件。综合来看，强化对数据使用的安全保护、扩大央行征信系统的征信范围和加强信息披露，是反欺诈体系发展完善的当务之急。

数据安全是第一道防火墙

数据是反欺诈的根本前提，无序且不受监管的数据使用却是欺诈产业得以“壮大”的重要基础。因此，个人数据在使用过程中的保护问题对于反欺诈体系的建立具有至关重要的作用。一方面，需要从国家立法层面厘清公民个人数据的使用权限和范围，明确一切未经用户授权的二次使用均属非法行为，进而从源头上掐断欺诈产业的数据来源。另一方面，企业要加强数据保护的技术研发，使所有数据能够按需利用不至于外泄，特别是在和第三方的开放合作中，也应该通过相关机制来保障数据的安全使用，构建数据使用的安全屏障。

扩大央行征信系统的征信范围

数字金融的健康发展也离不开央行征信系统的有力支撑。一方面，要将数字金融行业的征信数据纳入央行征信系统，丰富央行征信系统的数据来源，进一步提高央行征信数据的权威性和多样性。目前央行已经获准百行征信有限公司正式开展个人征信业务，这有望解决数字金融领域的征信缺失问题，也为下一步数字金融行业征信数据和央行征信系统共享打下了坚实基础；另一方面，获准数字金融企业使用央行征信数据，目前大多数互联网消费金融机构尚无法运用央行征信系统数据，使其在贷前应用大数据分析时，因缺失信贷信息而易面临较大信用风险。甚至许多欺诈者就是因为金融科技机构无法使用央行征信数据，肆无忌惮地进行欺诈。

加强信息披露

充分的信息披露将极大程度地提高违约成本，使数字金融行业的诚信体系更容易建立。一方面要允许、鼓励众多主体共享信息，从而有丰富、透明和标准化的交易信息供市场评估筛选和有效决策。另一方面需要有充分、强制的信息披露。这不仅需要资金融入方或者说产品提供方主动披露信息，交易过程也会倒逼信息透明、强制交易双方互动筛选出更多的信息。

技术是支撑

欺诈和反欺诈是对立的两面，中性的技术决定了其既可以被不法分子利用行诈骗之事，也可以服务于匡扶正义的反欺诈事业。为了更好利用技术手段打击诈骗行为，一方面，我们要不断优化反欺诈模型和系统构建，综合运用多种技术手段对欺诈行为进行精准打击；另一方面，要将先进的技术在行业内共享，优秀企业的技术输出值得鼓励。

不断优化反欺诈模型和系统构建

反欺诈模型和系统架构是构建反欺诈方案的核心要素。首先反欺诈模型是核心竞争力，特别是基于机器学习技术构建的反欺诈模型是重要的发展趋势，它能够分析各类用户的行为特征，并计算出金融业务不同环节中的风险概率，从而有效识别风险。其次，系统架构直接影响欺诈行为的识别效果，这对系统的处理速度和稳定性提出更高的要求。

升维和跨界

随着欺诈手段逐渐升级，反欺诈技术也需要升维发展。一方面，要多种技术手段组合运用，构筑多维度的反欺诈模型，比如将数据采集、数据分析、机器学习等技术结合应用多维度整合、分析数据信息，有效治理欺诈行为；另一方面，要从跨行业的视角出发，对欺诈行为进行打击。行业之间跨界融合发展是大势所趋，只有从跨行业角度出发，多维度地甄别、审查，才能实现对欺诈行为的精准打击。

实现技术输出

如前所述，优化模型、系统构建需要大量的人力和物力，拥有较大规模和较强实力的企业才能

面面兼顾。目前部分中小企业限于技术水平、资金实力，反欺诈能力薄弱，但是技术成熟、反欺诈能力较强的企业可对中小企业赋能，补平短板，共谋和平的网络安全环境。实力较强的大企业要实现技术输出，才能增强整个行业的反欺诈能力建设。

机制是保障

欺诈泛滥一方面是由于不法分子利欲熏心，另一方面也是我们的现行机制漏洞给不法分子提供了犯罪的可乘之机。要从根本上弱化欺诈的动力源，需要我们不断优化机制。首先，要提高金融科技企业的门槛，做到扶优限劣。其次，需要多方共同合作，构建由监管部门、行业协会、金融机构、科技企业共同参与的反欺诈联盟。

提高金融科技企业的门槛

数字金融的欺诈乱象很大程度上源于行业内提供服务的企业良莠不齐：一些规模小、实力弱的企业，部分打着金融科技旗号的假金融、野金融公司的庞氏骗局、吸金等非法行为，使整个行业笼罩了一层阴影。因此，提高金融科技企业的门槛成为优化行业生态的关键之举。这需要监管部门要建立一套详细的指标体系对金融科技企业进行评价认定，同时在政策上对真正的金融科技企业进行引导和扶持，让优秀的企业有快速成长和脱颖而出的环境，做到扶优限劣，促进行业高质量发展。

需要多方合作产生合力

数字金融欺诈多样化、产业化、隐蔽化、场景化的特点，决定了反欺诈方式必须从孤军奋战走向联合打击。这种联合打击集中表现在两个方面：一方面，构建由监管部门、行业协会、金融机构、科技企业共同参与的反欺诈联盟，建立数据、技术、人才等方面的合作交流机制，强化同业间风险联防与合作，提高违约成本。另一方面，目前数字金融行业的消费者保护存在很大程度的缺失，维权途径和渠道不畅，因此，要加强行业层面对消费者的权益保护，可以联合建立客户权益保护中心，建立行业风险缓释与互助机制。

5 附 件

- 附件一：网络金融欺诈行为名词表
- 附件二：数字金融反欺诈技术名词表

附件 1　数字金融欺诈行为名词表

1. 盗号（第三方支付）

第三方支付账号一般都关联着用户的银行卡、信用卡等信息，且多数第三方支付平台为了保证客户体验，只需首次授权，之后只要登陆网络支付账号就能使用信用卡或者借记卡付款，无须再次关联。所以第三方支付账号一旦被盗，将使用户的财产信息直接暴露在犯罪分子面前。犯罪分子通常通过木马病毒植入、钓鱼网站、拖库撞库等手段盗取用户网络账号。

2. 洗钱（第三方支付）

第三方支付账号一般可以关联多家银行的账户信息，利用第三方支付账号“漂白”通过非法手段获取的赃款相对容易。例如犯罪分子以前以银行对银行的方式进行转账，易被发现也便于追查，现在犯罪分子先把钱转到第三方支付平台，然后分转至多个银行账户取现则隐蔽性更强。尤其一些网络支付平台在用户注册账户时对其注册身份没有尽到核查义务，导致账号非实名，有些账号甚至可以任意买卖，加剧了第三方支付沦为洗钱通道的风险。

3. 保险互助平台欺诈

借助互联网手段，实现保险互助，降低保费、惠及民众，是网络保险发展的初衷，但由于一些制度设计缺陷，为不法分子实施诈骗留下操作空间。借互助之名，行非法集资之实的“假互助平台”是一种典型的欺诈手法。另外，平台还有可能通过篡改投保人数、投保时间、投保人身份、挪用互助资金等手段侵害投保人利益。

4. 理赔欺诈

网络保险不仅把互联网作为一种销售手段，同时也基于互联网业态创造了全新的保险险种，如退货运费险、账户安全险、延保险等，同时也滋生出很多恶意骗保的欺诈行为。比如电商平台的运费险，如果买家和卖家合谋，一单几毛钱的保费，就能骗取保险公司几十元的赔偿；再比如账户安全险，也有黑产团伙利用虚假账户恶意投保，通过骗保的方式获取巨额利息。

5. 网贷平台欺诈

网贷平台欺诈主要分为“伪平台”欺诈、模式风险、中立帮助行为三类。“伪平台”即不法分子从一开始便抱着“卷钱”、“吸金”心理，以网贷平台之名，行集资诈骗之实。模式风险是平台

本没有欺诈的意图，但运营模式客观上触碰法律红线且易发展成问题平台，比如自担保平台和债权转让平台。中立帮助行为主要是指网络中介平台在“贷款人”信息核查方面不能尽责或者明知信息不实仍为其提供互联网接入、广告推广、支付结算等帮助行为。

6. 冒用身份

贷款人在网络平台提供的身份信息、财产证明等信息极易造假，不法分子通过假招兼职、冒充客服、发送木马链接等手段非法获取个人信息，冒用他们身份骗贷或套现，事后由被害人承担损失。

7. 多头借贷

多头借贷即同一贷款人在多家平台提出信贷要求，多头借贷行为使违约风险增高，甚至一些恶意骗贷的欺诈用户开始就没有计划还款。

8. 套现欺诈

网络借贷滋生出专业中介和贷款业务，一方面，一些资质不好的人会联系中介，由中介包装身份（如挂靠工作单位、提供虚假财力证明等）后进行套现或贷款；另一方面，随着各公司风控能力日趋成熟，不少犯罪分子打着“中介”的幌子，进行套现欺诈。

9. 刷单

网络商户贷款基于电商卖家的历史交易信息对其进行批量授信，商户信息（包括交易信息）的真实性与商户的还款能力、还款意愿息息相关。商户刷单行为夸大了交易量，虚构了交易额，一些原本不能获得授信的商户通过刷单获得信用额度，一些原本只能获得较低授信额度的商户通过刷单获得了超过其实际能力的高额度授信。

10. 营销欺诈

营销欺诈即俗称的“薅羊毛”，羊毛党是一个分工明确、合作流程成熟的产业链，不法分子利用电商的营销漏洞，通过 QQ 群、微信群、论坛等组织大家薅羊毛，部分“羊毛党”与商家勾结，虚构交易，骗取电商平台的营销费用。

11. 转卖套现

套现者采用消费金融产品支付购买手机、数码产品或虚拟商品（例如充值、机票、门票）等易变现商品，交易完成后通过咸鱼等二手交易平台转让出售，以此套取现金。

12. 退款套现

套现者使用消费金融产品支付购买产品后，再通过现金退款等方式直接获取现金。

13. 虚构交易套现

买卖双方相互勾结，虚构交易或者虚抬价格，不法商户扣除好处费后与套现者直接现金结算。

14. 拖库

拖库原指从数据库导出数据，在网络欺诈领域，指黑客入侵后非法窃取网站数据库。

15. 撞库

撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登录其他网站后，得到一系列可以登录的用户。

16. 洗库

洗库，即对数据库中的资源进行层层利用，把里面的资源进行全方面的剥夺利用。

17. 钓鱼网站

钓鱼网站通常指伪装成银行及电子商务，窃取用户提交的银行账号、密码等私密信息的网站。

18. 木马

也称木马病毒，是指通过特定的程序（木马程序）来控制另一终端设备。

附件 2 数字金融反欺诈技术名词表

1. 大数据分析 （Big Data Analysis）

大数据指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产。大数据分析是指运用可视化分析、数据挖掘算法、预测性分析能力、语义引擎、数据质量和管理、数据存储等方法对大数据进行分析的过程。

2. 设备指纹 （Device Fingerprint）

设备指纹是指通过用户指纹为每个用户账户建立唯一的 ID，将用户的网络行为、设备、数据等综合信息建立稳定联系，保证用户安全。设备指纹技术可以用于包括账户安全、支付安全、营销安全在内的交易全生命周期监控。

3. 网络爬虫 （Web Crawler）

网络爬虫技术既可以用于用户运营商数据、信用卡数据、网络交易数据等各类数据等的爬取，也可以应用于司法老赖名单、网络核查数据的爬取。

4. 黑名单筛选 （Blacklist Screening）

黑名单筛选是针对注册用户反欺诈的技术手段。根据用户注册时填写的姓名、身份证号、手机号、银行卡号等要素信息，加上平台通过 SDK 抓取到的设备指纹和 IP，进行多维度筛选，与黑名单进行匹配，命中即拒绝。

5. 生物识别 （Biometric）

生物识别技术如声音识别、人脸识别等，是指对用户特定生物特征进行检测和识别的一种技术手段，通过比对用户的生物特征信息，判断用户身份，主要用于用户身份的核实等场景，防止出现用户账户被盗用的情况。

6. 人脸识别 （Face Recognition）

它是基于人的脸部特征，对输入的人脸图像或者视频流进行识别的技术。首先判断其是否存在人脸，如果存在人脸，则进一步的给出每个脸的位置、大小和各个主要面部器官的位置信息，并依

据这些信息，进一步提取每个人脸中所蕴涵的身份特征，并将其与已知的人脸进行对比，从而识别每个人脸的身份。

7. 虹膜识别 （Iris Recognition）

它基于眼睛中的虹膜进行身份识别。其核心是使用模式识别、图像处理等方法对人眼的虹膜特征进行描述和匹配，从而实现自动的个人身份认证。虹膜识别的主要步骤包括虹膜图像的获取、预处理、特征提取与编码和分类。

8. 生物探针 （Biological Probe）

它可以通过客户端等途径采集到用户在使用过程中的多项指标（如按压力度、设备仰角、手指触面、线性加速度、触点间隔等），基于这些行为的历史数据，通过机器学习计算专属行为模型，用于识别是否为本人操作。

9. 地理位置识别 （Geographic Location Recognition）

地理位置识别是一种通过真实地理位置识别基于位置欺诈行为的技术手段。地理位置识别利用包括 IP、基站、WiFi、身份证、手机号及银行卡等多维度的地理位置信息的信息库，精准定位网络访问者的信息，包括城市、经纬度及网络类型等，从而识别欺诈行为。

10. 活体检测 （Vivo Detection）

活体检测技术主要通过要求用户做特定动作或朗读特定内容，对用户是活人还是机器进行判断和检测，是防范欺诈团伙批量攻击的一种有效手段。

11. 文本语义分析 （Text Semantic Analysis）

文本语义分析主要用于对文本类数据的解析和挖掘，从用户评论等文本内容中提取用户特征。

12. 关系图谱 （ Map of Relationship）

关系图谱是利用图数据库，从特定维度对不同用户和不同操作行为之间进行关联和计算，从而发现不同用户和不同操作之间的关联关系，可以用于团伙特征检测等场景。

13. 用户画像 （User Profile）

用户画像是一种通过精准识别用户而反欺诈的手段。用户画像根据用户社会属性、生活习惯、消费习惯等信息抽象出标签化的用户模型。构建用户画像的核心工作是给用户贴标签，而标签是通过对用户信息分析而来的高度精炼的特征识别。

14. 有监督机器学习 （Supervised Learning）

有监督机器学习是反欺诈检测中最为广泛使用的机器学习模式。机器学习通常从有标签数据中自动创建出模型，来检测欺诈行为。其中包含的学习技术分别有决策树算法，随机森林，最近邻算法，支持向量机和朴素贝叶斯分类。

15. 无监督机器学习 （Unsupervised Learning）

无监督机器学习是无需依赖于任何标签数据来训练模型的机器学习模式。其可以通过利用关联分析和相似性分析，发现欺诈用户行为间的联系，创建群组，并在一个或多个其他群组中发掘新型欺诈行为和案例。

16. 半监督机器学习 （Semi-Supervised Learning）

半监督机器学习是有监督学习与无监督学习相结合的一种学习方法。半监督学习使用大量的未标记数据，以及同时使用标记数据，来进行欺诈识别工作。

17. 区块链 （Block Chain）

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。区块链去中心化、去信任的机制能够在预防性反欺诈领域进行有效应用。

18. 用户行为序列 （Behavioral Sequence）

用户行为序列也叫“基于时间序列的用户行为”，是某一时间段内，按照时间先后顺序记录的用户从事某种活动的每一步行为。

研究团队

孟昭莉	京东金融研究院院长
李　萌	京东金融研究院产业研究中心主任
唐艳红	京东金融研究院研究员
龚　谨	京东金融研究院研究员
许　晨	京东金融研究院研究员

业务支持团队

风险管理部	消费金融部	企业金融部	公共事务部
沈晓春	程建波	王越国	唐　杰
窦祚深	赵　飞	杜　强	
荆文宇	郭　晓	关　鹏	
孟繁星	王　檬	江　峰	
荆　磊	斯德华	高　歌	
		满运甫	

顾问团队

杨　东	中国人民大学金融科技与互联网安全研究中心主任、教授
秦玉海	中国刑事警察学院网络犯罪侦查系主任、教授

数字金融反欺诈白皮书

2018年

京东金融 JD Finance

中国人民大学 金融科技与互联网安全研究中心

中国刑事警察学院 NATIONAL POLICE UNIVERSITY OF CHINA