百融云创科技股份有限公司
地址：北京市海淀区科学院南路2号融科资讯中心
C座北楼20层
电话：010-62508053
网址：http://www.100credit.com

百融云创
Bairong, Inc.

反欺诈
行业调研白皮书

百融云创科技股份有限公司

2019年5月

目　录

图表目录

前　言

“金融欺诈”定义为使银行或者非银行金融机构发生错误认识为目的的故意行为，贷款申请人完全没有还款意愿，通过制造假相、隐瞒事实真相等方式使金融机构相信贷款申请人具备还款意愿与能力，从而获取金融机构贷款。贷款申请人的欺诈行为是金融行业中面临最具威胁的风险之一。

在传统信贷体系中，银行为主要放贷机构，而彼时传统的黑产，主要通过为客户包装、伪装资料等手段来骗取银行的授信。2012 年后，随着消费金融、P2P、小额现金贷等业务为代表的互联网金融的兴起，黑产在欺诈组织、技术、手段上都在不断更新，欺诈行为更是渗透到了信贷的各个环节。截至 2018 年末，黑产从业人员人数达到百万级，造成金融机构的损失达到千亿级别。同时金融信贷业务领域中，欺诈风险的高低与信用体系的完善程度有着密不可分的关系，据统计，截止 2018 年 6 月底，中国人民银行征信报告（以下简称“人行征信”）覆盖了 9.6 亿自然人，其中有信贷记录的群体不到 5 亿。有大量非持牌金融机构未能被纳入人行征信体系，也因传统信贷服务专注于较优质客群，大量长尾客户并未被银行服务过，所以无法仅通过人行征信报告全面评估贷款人风险。

由于信用体系完善程度的差异，不同市场对欺诈和信用风险的关注度也有较大差异，在美国的金融信贷领域，欺诈风险跟信用风险的成本支出比例约为 1：9；而在中国，欺诈风险与信用风险的成本支出比例平均约为 4：6，其中持牌金融机构因其服务的客群相对优质，欺诈与信用风险支出比例约为 3：7；非持牌金融机构，如 2017 年以前只关注客户欺诈风险的现金贷机构，目前来看行业成本支出比例约为 7：3。可以看出，在相对成熟的市场，信用风险是金融机构重点关注的方面。但因中国互联网金融行业兴起不久，在现阶段，针对中国市场上充斥的大量黑产，对欺诈风险进行深入解读具有重要意义。

本报告将从目前欺诈行业的现状及欺诈的不同目的对欺诈风险进行分类并逐一详细介绍。同时从百融云创科技股份有限公司（以下简称“百融云创”）自身数据所观测到的欺诈表现对欺诈黑产进行全方位刻画，并对目前信贷行业发展受限的痛点提出我们的看法。希望帮助市场参与机构从不同角度了解黑产，助力行业更快更好的发展。

百融行业研究中心（以下简称“百融行研中心”）是百融云创所属研究机构，凭借公司服务银行等金融机构的丰富经验以及超强的大数据处理和建模能力，高度贴近产业发展实践，深度整合国内外研究力量，不断形成高水平研究成果，为企业、产业和整个国民经济的转型升级提供智力支持，“因为专业，所以卓越”。

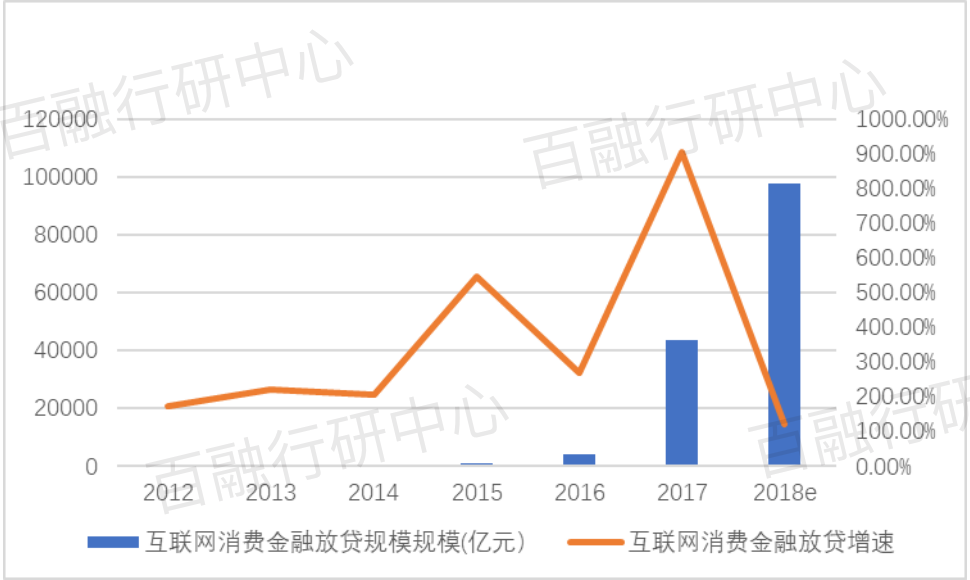
01 欺诈行业现状

一、欺诈行业现状

1.1 互金行业市场规模

中国互联网金融自 2012 年起一直处于高速发展的阶段，2012 年贷款金额为 18.6 亿元，2017 年达到 43,847.3 亿元，每年放款增速均保持在 200% 以上，其中 2015 年的增速相比前三年有明显的提升，达到 646%，2017 年增幅最大，达到 904%。

图 1：中国互联网消费金融放贷规模及增速

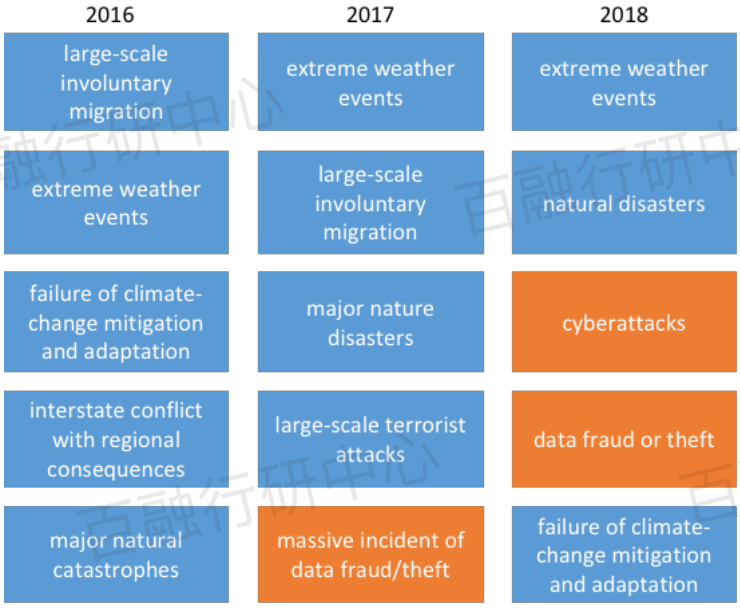


数据来源：艾瑞咨询，数据整理：百融行研中心

1.2 黑产市场

首先在全球范围来看，诈骗和数据泄漏随着互联网和金融市场的发展，也逐渐变为整体国际市场风险问题的核心一环。在世界经济论坛发布的《2018 年全球风险报告》中指出，在 2016 年到 2018 年全球风险排名 TOP5 变化表中，2017 年数据诈骗或者数据泄露的风险开始初露头角排名第五，而到 2018 年，网络黑客攻击和数据安全已上升至第三名和第四名。这说明，网络安全已经成为除了自然灾害以外，最大的风险所在。

图 2：Top 5 Global Risk in Terms of Likelihood



数据来源：世界经济论坛，数据整理：百融行研中心

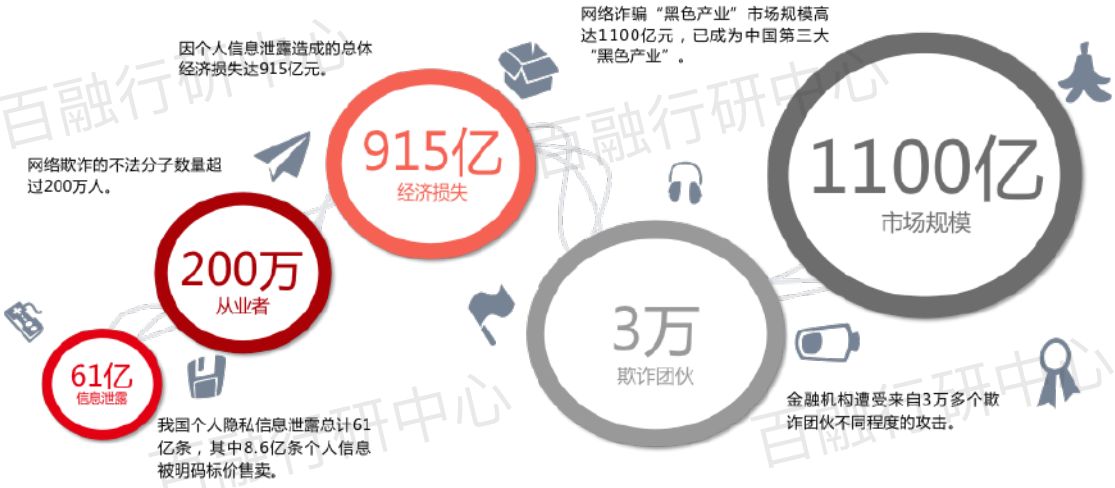
而在中国，网络黑产热点也居高不下，逐渐成长为侵蚀经济和社会的毒瘤。例如在《2018 网络黑灰产治理研究报告》中显示，全球每 3 起网络攻击中就有 1 起发生在中国。其中电信诈骗增长速度瞩目，为 20% 至 30%。中国网络黑产中每年都有将近 6.88 亿网民受到垃圾信息、数据泄露以及网络诈骗的侵害。

图 3：中国网络黑产特性

数据来源：南都大数据研究院，数据整理：百融行研中心

特别的，从黑产市场本身角度出发（图 4），截至 2018 年，黑产造成的信息泄漏预计在几十亿条上下，从业人员超过 200 万，涉及欺诈团伙超 3 万个。其中因个人信息泄漏造成的总体经济损失可能已超 900 亿元，目前黑产市场规模预估已逾千亿级别。

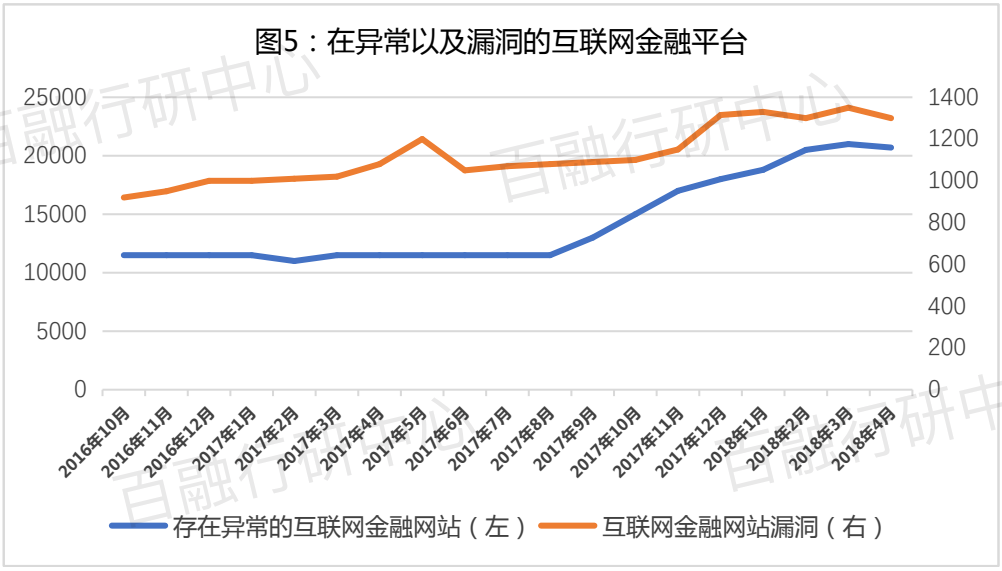
图 4：黑产市场现状



数据来源：公开信息，数据整理：百融行研中心

对于互联网金融平台来说，据国家互联网技术专家委员会统计，2017 年 8 月开始，存在异常的互联网金融网站数量开始明显增多。截止至 2018 年 4 月，其互联网金融风险分析技术平台发现了 21,624 个存在异常的互联网金融网站和 1,362 个互联网金融漏洞。

图5：在异常以及漏洞的互联网金融平台



数据来源：国家互联网金融安全技术专家委员会，数据整理：百融行研中心

2012 年以前，国内经营信贷业务的机构以银行为主。传统的黑产，主要通过为客户包装、伪装资料等手段，骗取银行的授信。2012 年后，随着消费金融、P2P、小额现金贷等业务为代表的互联网金融的兴起，欺诈团伙有了更广阔的土壤。随着欺诈组织、技术、手段的不断更新，欺诈行为逐渐渗透到金融营销、注册、登录、贷款申请、支付以及交易等各个环节。

图 6：金融欺诈高发环节

数据来源：百融行研中心

最后，对于近两年网络黑产的发展方向，我们可以从五个方面来概括：第一，由于欺诈信息的不断丰富多元，使得黑灰产欺诈方式和技术更加精准化；第二，欺诈分子随时关注国家政策和监管动向，做到政策稍一调整，马上转变产业策略；第三，为了提高诈骗效率，诈骗对象从个人向单位转移；第四，欺诈团伙的开户机构目标逐渐从大型银行转向中小银行和第三方支付机构，利用中小机构风控相对薄弱的特点，减少自身暴露的风险；第五，欺诈分子资金转移过程快，层级环节复杂，例如流窜作案、跨国诈骗等。

图 7：网络黑产发展方向

数据来源：百融行研中心

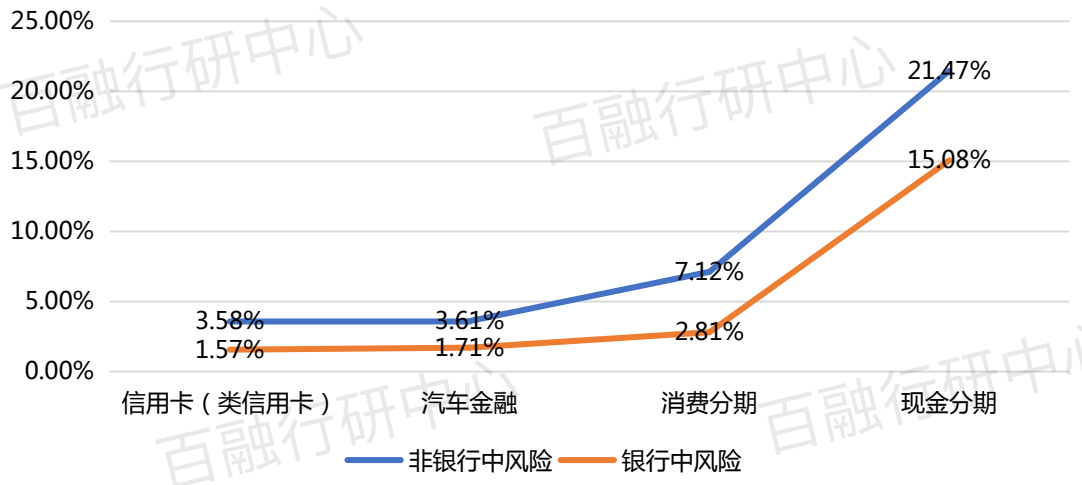
1.3 欺诈客群画像

百融云创从欺诈类客群着手，先从行业、区域、性别以及年龄进行观察，再从非银和银行类机构客群表现着手，观察到不同分类体系中，欺诈风险存在不同的分布特性。

1.3.1 欺诈客群行业分布

从行业来看，我们先将现有客群分为信用卡（类信用卡）、汽车金融、消费分期以及现金分期四个行业（图 8）。其中，信用卡（类信用卡）和汽车金融客群由于客户资质相对较好，所以整体的欺诈数据命中率是所有行业分类中最低的。第二档次的为消费分期，可以看到，由于消费分期客群依托具体消费场景，整体违约水平稍好于现金分期，但同时，由于客户层次覆盖范围较信用卡（类信用卡）和汽车金融更广，涉及的机构层次种类更多，导致客群质量相对信用卡（类信用卡）和汽车金融类客户更低一些。最后，现金分期类客群整体欺诈风险是四个行业中最高的，这里的现金分期包含所有种类的现金分期产品，总体客群资质较为下沉，有时还会涉及个体工商户等相对更复杂的客群，不确定性较大，所以可以看到整体欺诈数据命中率最高。另外，从非银和银行机构的角度来看，四类客群非银机构欺诈比例都要高于银行类机构，说明总体非银类机构客群是明显差于银行类机构的，符合市场规律。相比之下，差别较大的为现金分期（非银和银行差值为 5.5% 左右）以及消费分期（非银和银行差值为 4.3% 左右），说明相比其他两个行业，这两类客群在非银和银行机构中两极化更明显，差异性更大。

图 8：欺诈客群按行业分布



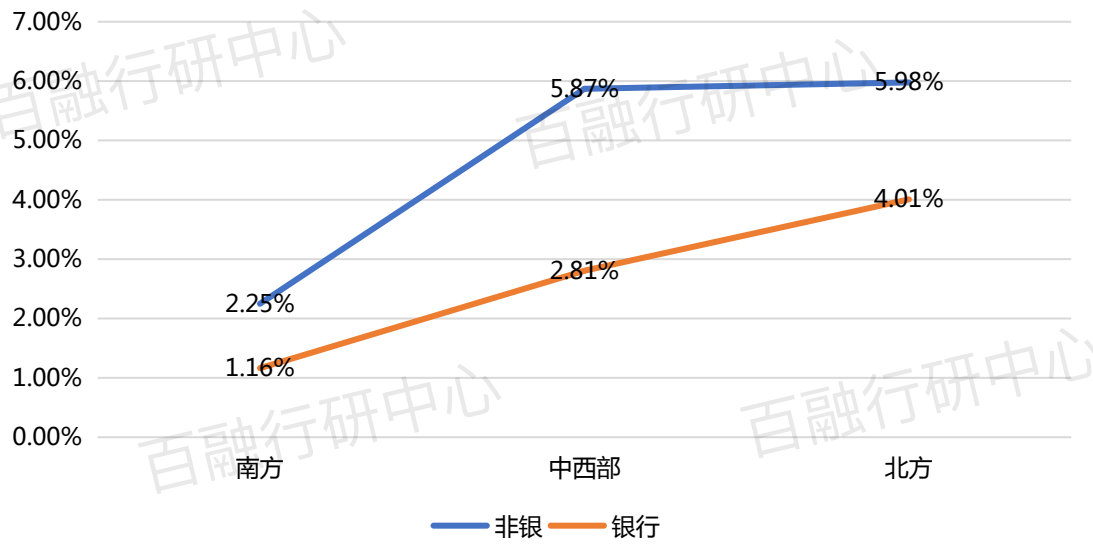
数据来源：百融行研中心

1.3.2 欺诈客群区域分布

从区域分布来看（下图9），我们将总体区域分为了南方、中西部以及北方。其中北方地区包括黑龙江、吉林、辽宁、北京、天津、河北、山东、河南与山西等地；中西部地区包括陕西、四川、云南、贵州、广西、甘肃、青海、宁夏、西藏、新疆与重庆等地区；南方地区包括江苏、安徽、浙江、上海、湖北、湖南、江西、福建与广东等地区。可以看出，北方和中西部地区欺诈风险相对较高，南方地区欺诈风险相对较低。

同时我们还可以观察到，中西部非银和银行之间欺诈标签命中率差距是最大的，达到2倍以上，说明两种机构在中西部地区对于客群区分要更加明显，亦或此区域银行类机构对于自身目标客群的把控更加明确或者严格，而非银机构对于客群纵深做的更加深入。

图9：欺诈客群按地域分布

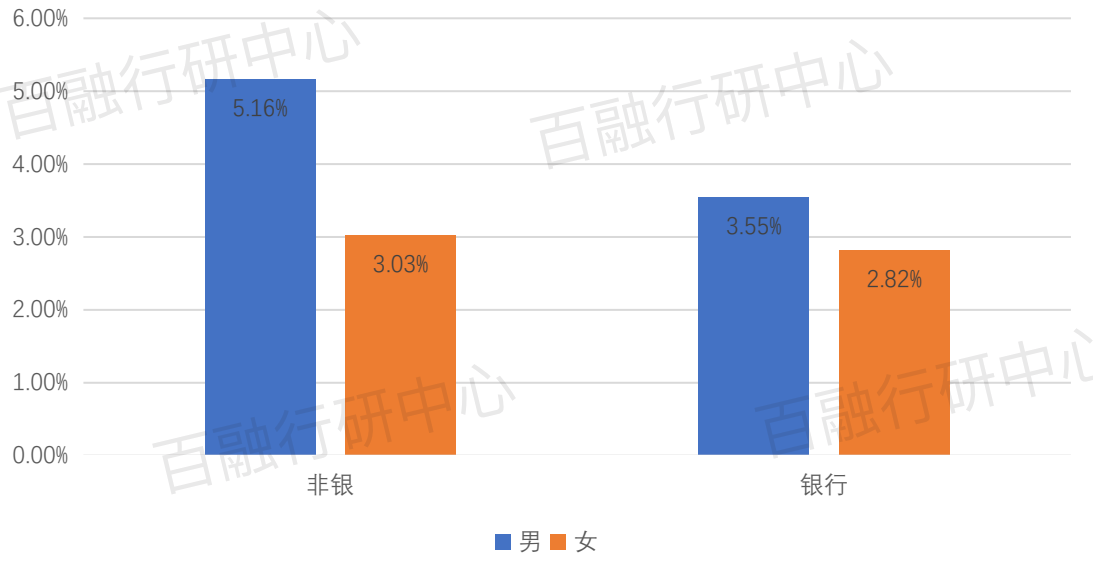


数据来源：百融行研中心

1.3.3 欺诈客群性别分布

从性别分布来看（图10），男性欺诈风险是大于女性的。究其原因，通过查看相关数据，我们发现，在非银机构中，男性中高风险命中率要明显高于女性，而在银行体系中，男女各项风险标签命中情况区别并不明显。说明在客群资质更加下沉的非银机构中，中高风险男性客户占比更多。

图 10：欺诈客群按性别分布

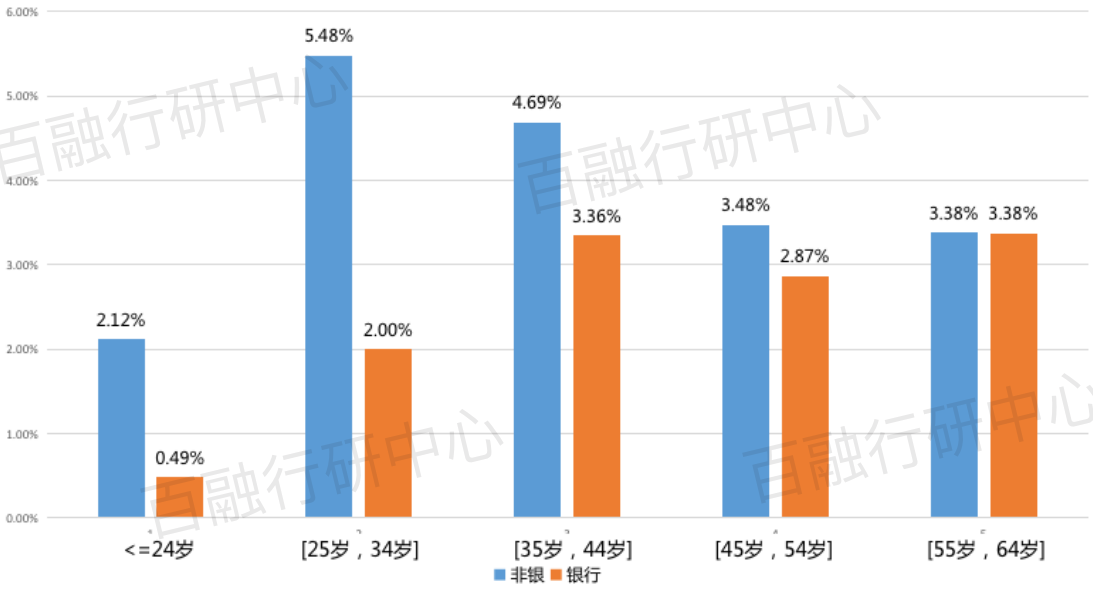


数据来源：百融行研中心

1.3.4 欺诈客群年龄分布

从年龄分布来看（图 11），我们以十岁为一个档次，将年龄分为了 5 组进行观察。从结果上看，欺诈命中情况分布较为均匀，除 24 岁以下人群受人群特质影响，特别是对未涉入社会的年轻人借贷会受到限制，所以某些类型的欺诈标签对于这类人群的覆盖会有偏，而其他年龄段基本都在 3%-6% 的命中区间。首先不论哪个年龄段，非银客群命中欺诈标签的比例都明显高于银行类客户，特别是 25 到 34 岁这个年龄段，两种机构的客群欺诈命中率差别最大，在 35 岁以后两者差异逐渐收敛，也说明 25 到 34 岁本身客群相对其他年龄组来说风险较大，同时对于非银来说接受的客群资质更加下沉。

图 11：欺诈客群按年龄分布



数据来源：百融行研中心

1.4 欺诈分类

除了恶意套现、保险业骗保等层出不穷的欺诈手段，伴随着互联网时代的发展，个人信息泄露、黑产组织化问题更趋向于高额化、精准化、羊毛党，互联网欺诈等行为也在变得愈发猖獗。同时，传统风险与新型风险相互交织，各类欺诈手法不断翻新。观察整个行业，按金融欺诈种类划分，可以分为羊毛党、信贷欺诈以及盗刷盗号三类。

图 12：欺诈三大种类

数据来源：百融行研中心

简单来说，羊毛党是指利用金融机构发起的营销、优惠以及折扣等为招揽客户的活动机会，提品大规模地获取相关利益，致使正常客户无法获得益处，导致金融机构无法达成预期效果的群体。信贷欺诈是指通过冒用、盗用他人身份信息或者包装申请人资质以骗取金融机构贷款的行为。盗号盗刷即盗用持卡人资料或者相关账户信息，进行伪冒交易来实施诈骗的过程。

下面本文就分别对这三种欺诈类型做进一步解析。

02 羊毛党

二、羊毛党

羊毛党专注于市场上各类机构的营销活动，以低成本甚至零成本换取高额奖励，其主要活跃在 O2O 平台或电商平台。随着 2012 年以后互联网金融的高速发展，一些网贷平台为吸引用户常推出一些收益丰厚的奖励活动，如注册认证奖励、充值返现、投标返利等，在吸引潜在用户的同时，也催生了专门以此牟利的投机群体，他们也被称为“互联网金融羊毛党”，简称“互金羊毛党”。互金羊毛党跟一般的羊毛党不同，他们只关注互联网金融平台，主要在注册、登录等环节对平台进行攻击。

互联网金融平台为了吸引客户到自己的平台进行各项交易，投入大量资金推出各种新用户注册返利优惠活动。互金羊毛党利用手机黑卡到各互联网金融平台大量的注册新用户，平台的活动经费大量落入互金羊毛党的账户中，活动的效果大打折扣，有的平台甚至因为互金羊毛党薅羊毛而倒闭。

图 13：羊毛党 QQ 群

数据来源：百融行研中心

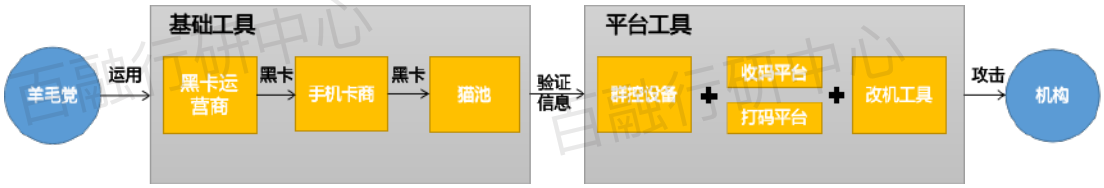
随着互联网业务的发展，互金羊毛党也由最初的单兵作战演变成为有组织的团体作战。不仅有专业工具、技能，且每个互金羊毛党群体都会有几名主要负责人，管理并指挥羊毛党统一作案。

据了解，互金羊毛党群体的负责人会直接跟网贷平台市场、渠道、风控甚至机构负责人进行商议，要求平台提供一笔大额资金，以确保该互金羊毛党群体不会对平台进行攻击。另一方面，我们也观察到部分网贷平台市场、渠道负责人可能会主动跟互金羊毛党联系，要求其在平台中进行大批量注册，造成平台用户数量短期内高速增长的假象，从而骗取互金平台负责人的信任。有了好的业绩，这部分网贷平台市场、渠道的负责人通常会选择跳槽到另一家规模更大、薪资待遇更好的网贷平台继续负责市场、渠道的工作。

互金羊毛党能够形成集团化的专业组织，依靠的是一条完整的黑产生态链，主要包括黑卡运营商、手机卡商、猫池厂商、收码平台、打码平台、改机工具以及群控工具等。

在具体操作流程上（见图 14），首先，“羊毛党”需要建立基础工具平台。一个完整的猫池基础工作平台中，黑卡运营商会通过各类途径获得手机黑卡，随后批量卖给手机卡商，手机卡商将手机黑卡插入猫池批量接收验证码。接着，在基础平台运作完成以后，验证信息会传输至平台工具模块；“羊毛党”会分别从收码平台和打码平台批量及部分自动化地收集验证码，其中收码平台会协助完成短信验证，而打码平台负责识别文字、图像、滑动等难度较大的验证码。同时，“羊毛党”会通过群控工具以及改机工具提升设备的整体利用率，甚至实现部分模块自动化操作。最后，在整套自动化工具整合好后，“羊毛党”便可对相关机构进行批量攻击了。

图 14：羊毛党产业链运作流程



数据来源：百融行研中心

接下来我们将介绍羊毛党核心产业链条的组成及运作方式。

2.1 黑卡运营商

手机黑卡是指没有在运营商进行实名认证，被不法分子利用进行薅羊毛攻击、传播淫秽色情信息、实施通讯信息诈骗、组织实施恐怖活动等违法犯罪活动的移动电话卡。

黑卡运营商通常与三大运营商代理勾结，或者黑卡运营商本身就是三大运营商代理。他们在获得大量手机卡后通过加价转卖给下游手机卡商赚取利润。其黑卡主要来源有：实名卡、物联网卡、海外卡以及虚拟卡。

（1）实名卡：实名卡主要是通过拖库撞库、木马、钓鱼等方式从网上收集大量身份证信息，并通过黑卡运营商批量验证得到的。

（2）物联网卡：物联网卡是由三大运营商业提供的 4G/3G/2G 卡，硬件和外观与普通 SIM 卡相似，但采用专用号段，并加载针对智能硬件和物联网设备的专业化功能，满足智能硬件和物联网行业对设备联网的管理需求以及集团公司连锁企业的移动信息化应用需求。

主要有基础通信、财务信息查询、终端状态查询、业务统计分析四大功能。物联网卡无需进行实名验证，由企业申请办理，一般仅需提供营业执照，实际操作中，营业执照通过财务公司操作，大概需要花费 1,000 元左右即可成功注册，部分运营商对营业执照审核不够严谨，甚至会为灰产[①]定制专用的物联网卡套餐。这种物联网卡

① 灰产：一种介于正当行业与不正当行业之间的产业。

多为免月租或者 1 元月租，根据能否接听电话，分为短信卡（也称“注册卡”）和语音卡。

（3）海外卡：在国家实行实名制后，黑卡运营商直接从海外购入手机卡，这些卡无需实名认证，花费很少，非常切合黑产利益。

（4）虚拟卡：由虚拟运营商提供的电话卡。虚拟运营商是指拥有技术、设备供应、市场营销等能力，与传统三大运营商在某项或者某几项业务上形成合作关系的合作伙伴。虚拟运营商就像是代理商，他们从移动、联通、电信三大基础运营商那里承包一部分通讯网络的使用权，然后通过自己的计费系统、客服号、营销和管理体系把通信服务卖给消费者。

2.2 手机卡商

手机卡商从黑卡运营商那里大量购买手机黑卡，将手机黑卡插入猫池设备并接入收码平台，然后通过收码平台接收各种验证码业务，根据业务类型的不同，每条验证码可以获得 0.1 元 -0.3 元不等的收入。

2.3 猫池厂商

猫池就是将相当数量的 Modem 使用特殊的拨号请求接入设备连接在一起，可以同时接受多个用户拨号连接的设备。插上手机卡就可以模拟手机进行收发短信、接打电话，可以实现对多张手机卡的管理。广泛应用于大量具有多用户远程联网需求的单位或需要向从多用户提供电话拨号联网服务的单位。如邮电局、税务局、海关、银行、证券商、各类交易所、期货经纪公司、工商局、各类信息呼叫中心等。在黑产链条中，猫池厂家负责生产猫池设备，并将设备卖给手机卡商使用。

图 15：猫池

数据来源：网络公开信息，数据整理：百融行研中心

2.4 收码平台

短信验证码是企业给消费者（用户）的一个凭证，通过短信内容的码来验证身份。主要应用在注册、登录等场景。收码平台是负责连接手机卡商和羊毛党等有手机验证码需求的群体，提供软件支持、业务结算等服务，通过业务分成获利的平台。一般会提供给使用者客户端、API 两种对接方式，手机客户端以支持各种手机业务，API 能够对接到自动化工具、脚本中，实现批量注册。黑产从业者从收码平台接收一个验证码需要支付 0.1 元 -0.3 元。

收码平台的使用者首先要将自己的项目在系统中进行报备后才能正常收取验证码，使后台能够正确的分配手机号码，避免手机号重复使用。如果遇到某些平台注册过程需要接收多次验证码，则需要在收码平台上进行特殊报备。平台会将收发集成一个流程，供使用者批量化操作。有些网贷平台使用语音验证码，因此收码平台也产生了相应收取语音验证码的服务。

收码平台数量较多，活跃的约有数十家，比较知名的接收码平台有：爱乐赞、玉米（现菜众享）、Thewolf、星辰等，其中 Thewolf 和星辰可以接语音验证码。

图 16：收码平台

数据来源：百融行研中心

2.5 打码平台

收码平台主要负责接收验证码，打码平台则主要负责将验证码发送至网贷平台中。短信验证码能够通过收码平台自动化操作，但文字、图像、声音等验证码的技术难度较高，收码平台通常难以完全依赖技术手段实现

自动操作。国内的打码平台，以往主要依靠低廉的劳动力。他们对无法技术解决的验证码使用人工打码进行破解。这种方式广泛传播到了大量第三世界国家，导致全球有近百万人以此为生。打码工人平均每码收入 1-2 分钱，熟练工每分钟可以打码 20 个左右，每小时收入 10-15 元。

随着技术的发展，打码平台也与时俱进，逐渐产生了使用人工智能打码的平台。如警方在 2017 年打击的“快啊答题”平台，其使用了伯克利大学的数据模型，引入大量验证码数据对识别系统进行训练，将机器识别验证码的能力提高了 2,000 倍，价格降低到了每千次 15-20 元。为撞库等需要验证的业务提供了极大的便利。

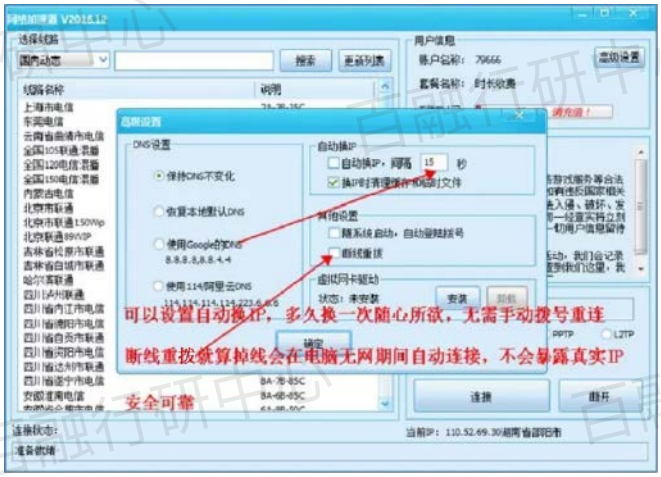
图 17：打码平台

数据来源：百融行研中心

在网络黑色产业链中，存在上百种撞库软件，往往都集成了打码平台的功能，即通过链接到打码平台实现对验证码的识别破解。值得注意的是，这些黑产链接的打码平台往往都采用了人工智能的深度学习技术进行机器训练，导入大量的数据，使之能够有效识别字符、图片等验证码，大幅提升验证码的破解率。

为了防止平台对相同 IP、设备发起的打码行为进行限制，部分打码平台采用了黑科技“秒拨”。“秒拨”可以调用国内甚至国外的 ADSL 宽带动态 IP 资源，只要通过简单配置，就可以实现 IP 的“自动切换”、“秒级切换”、“断线重拨”、“清理 COOKIES 缓存”、“虚拟网卡 (MAC) 信息”、“多地域 IP 资源调换”等可规避网站 IP 及相关防御策略的服务。

图 18：秒拨平台



数据来源：百融行研中心

2.6 改机工具

一般来说，机构平台在设备进行相关操作（例如注册、登陆等）对底层信息的探测以及定位会导致一部手机的使用受到了极大的限制，所以对于羊毛党来说，需要更多的手段来多次数多元化的运用相关设备，改机工具就是至关重要的一环。

其可以通过修改设备底层信息来帮助羊毛党规避机构平台对于“同一设备”的探测，简单来说，“一台手机 + 改机工具 = 无数台手机”。

2.6.1 改机工具原理和功能

（1）IOS 环境

对于 IOS 系统来说，底层基本原理运用的是逆向开发中的 HOOK 技术，通过修改替换系统方法回调的参数从而达到改机的目的。并且工具中的核心源码都是来自于一位国外的作者编写，改机工具的作者将其封装增加使用限制已达到盈利目的。

IOS 环境下改机工具的功能主要为全息备份、伪装设备信息参数、防越狱检测、模拟定位（部分改机工具有此功能）以及清理 Keychain[②]。

①全息备份是备份原始机器和应用信息，方便改机之后恢复原机信息。

② Keychain：IOS 系统中一个比较隐蔽和稳固的存储位置，一般不易被清除。

②伪装设备信息即指定一个应用 APP 进行伪装修改设备参数，一键新机之后，该应用中采集到的设备信息参数即为伪装好的设备信息。

③防越狱检测即开启防越狱检测之后，无法检测出这是一台越狱设备。因为安装改机工具必须需要越狱环境，所以对于安全性要求较高的应用 APP 越狱环境下会有很大的安全隐患。例如支付宝和微信，如果检测设备为越狱环境，就会禁止用户进行某些操作，比如指纹支付操作等。

④模拟定位即模拟地理位置，使应用采集到的经纬度地址与实际的经纬度地址不符。

⑤清理 Keychain 是清除应用对应的钥匙串（应用卸载不会清除）里面的信息。

下面以 AWZ 爱伪装为例，对 IOS 改机工具常用功能做展示：

图 19：IOS 改机工具功能展示

数据整理：百融行研中心

（2）Android 环境

Android 改机工具主要是通过 Xposed 框架完成的，改机工具都是运行在 Xposed 框架内的模块，Xposed 框架集成在 Xposed Installer APP 内，可通过不同设置来决定哪些模块是否生效（如图 20）：

图 20：Xposed 内含模块展示

数据来源：百融行研中心

如上图，选择对应的修改模块后，可以实现对 Android 手机的 IMEI、MAC、型号、制造商、定位等信息的修改与伪装。

2.6.2 改机工具预防效果

（1）百融谛听设备反欺诈简介

百融谛听设备反欺诈核心产品为设备指纹，也叫 GID。GID 是百融云创自主研发用于跟踪和分析设备的唯一标识，服务端根据采集到的非个人敏感特征信息，OSI 七层协议栈，网络特征，通过动态综合加权、相似度等算法生成唯一指纹 GID，一台设备终身一个全球唯一 GID。

百融谛听反欺诈对目前市场存在的改机工具涵盖能力如下：

图 21：百融谛听设备反欺诈应对主流改机工具效果

	iGrimace	NZT	海鱼魔器	007 改机	008 神器 A	应用变量	尖兵手机修改器	手机修改器	IMEI Changer Pro	xx 神器 4
应用图标										
谛听反欺诈能否识别	能	能	能	能	能	能	能	能	能	能

数据来源：百融行研中心

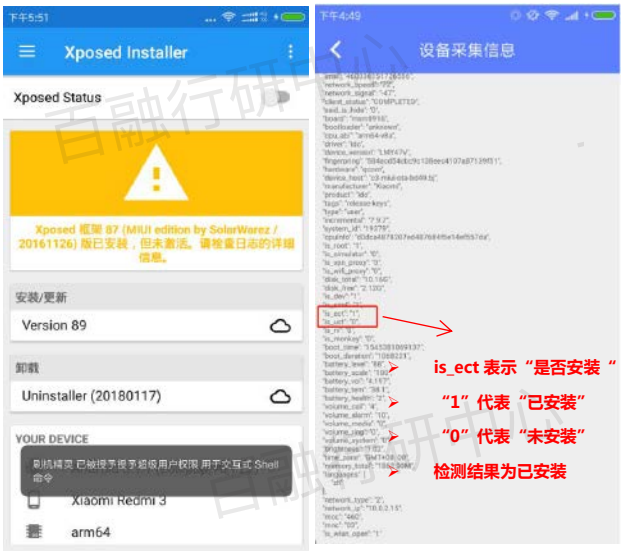
（2）改机工具识别展示

下面我们以 Android 设备为例来看下百融谛听设备反欺诈对改机工具的预防效果。

①改机工具安装识别

如图 22，左图中显示 Xposed 已经安装到该设备当中，右图则显示百融谛听设备反欺诈探测到了该改机工具的安装结果（“是否安装”字段显示的是“已安装”）：

图 22：改机工具“安装”状态识别



数据来源：百融行研中心

而如果设备在未安装改机工具的情况下，如图 23，左图中显示该设备中无 Xposed，右图显示百融设备反欺诈未探测到改机工具的安装结果（“是否安装”字段显示的是“未安装”）：

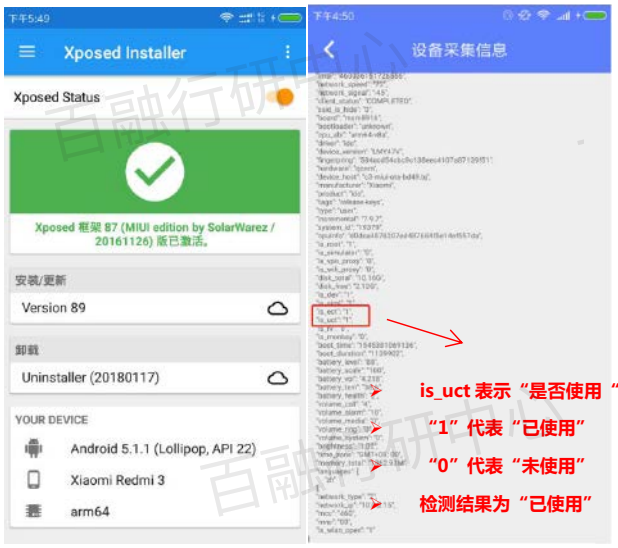
图 23：改机工具“未安装”状态识别

数据来源：百融行研中心

②改机工具使用状态识别

同理，对于已经安装改机工具的设备，百融还可探测其使用状态，如图 24，左图中该设备 Xposed 已经激活使用，右图中显示百融探测到了改机工具是出于激活使用状态的（“是否使用改机工具”字段显示的是“已使用”）。

图 24：改机工具“已使用”状态识别



数据来源：百融行研中心

③使用改机工具后百融设备指纹识别的稳定性（以“手机修改器”为示例）

首先正常情况下使用百融谛听设备反欺诈生成设备指纹以及相关设备信息，如图 25，此时设备指纹被识别为 ：“4443330001001536651675363450334 5”。

图 25：初始设备指纹编号

数据来源：百融行研中心

然后打开 Xposed Installer 选中“手机修改器”模块（如图 26），修改相关设备信息，例如 IMEI 值、机型、厂商、品牌等。

图 26：改机工具中的“手机修改器”模块

数据来源：百融行研中心

接着打开百融谛听设备反欺诈查看 GID 能否识别为原有设备。从图 27 左图和中图里，我们可以看到，“手机修改器”模块依次修改了设备的 IMEI 值（从“869055027340938”变为“9876543210”）、MAC 值（从“64:cc:2e:d6:46:96”变为“06:05:04:03:02:01”）、型号（从“Redmi 3”变为“vivo x20”）以及制造商（从“Xiaomi”变为“vivo”）四项信息。但是可以看到，GID 并没有因为设备基本信息的修改而无法识别原设备，在图 33 右图中设备指纹仍为：“44433300010015366516753634503345”。

图 27：GID 稳定性测试

数据来源：百融行研中心

2.7 群控平台

群控是指通过一台电脑或者手机设备控制批量手机的行为，可以分为线控和云控两种形式。线控是指信号发生器与被控制的手机设备通过线缆进行连接的；云控指手机搭载了云技术可以实现远程控制，可以用任意一台 PC 通过云端控制手机终端上的任何资料，随意调取自己所需的信息，或者使用另一部手机用 ID 登录云服务器。通过群控工具，可以实现一台终端对多台手机的控制，与改机工具进行搭配，可以在短时间内制造成千上万不同设备的信息，适用于羊毛党的批量攻击。

市面上较为常见的群控平台有通路云、侠客、李铁拐、大群控、巧布施、河马云群控等。这些群控平台能通过一台电脑控制 50 台以上的设备，同时部分群控平台能够提供增值服务，简单对比分析如下：

（1）河马云平台在群控基础上提供切换 IP、修改手机参数等改机功能，提升设备利用率，使平台集成自动化程度更高。

（2）QQ 群控提供配套猫池，配套养卡、养号工具，使群控账号更加接近真实账号。

（3）李铁拐提供精控、群控、云控三类服务。

精控系统是指在一台电脑上同时登陆多个账号，模拟真人操作，不需要手机，无法被检测，每个账号的 IP 都是独立的，可集自动加粉、群发信息、自动养号等功能于一体的营销管理系统。技术安全性大大的提高，防平台封 IP 号能力强。精控同时还搭配最新的 AI 图像识别技术，可针对高难度的图像识别验证码进行批量破解。每个精控平台仅需要 1 个普通工作人员即可维护，维护成本低、运营效率高。

群控系统是指通过一台或多台电脑，辅以群控软件，通过设备支架以及连线在本地同时控制多台手机，每个手机配置一个 IP，50 台设备大约需要三人进行链接及刷机的维护，运营效率较高，但防平台封 IP 号能力较强，同时控制 50 台设备的硬件成本大约为 5 万，包括 50 台手机（4 万）+ 软件、支架、HUB（1 万）。

云控系统是指通过手机搭配云控软件，外接第三方云服务，实现少量设备对多台虚拟设备的控制。云控通常需要 5 台本地手机设备，成本大概在 4,000-5,000 元左右，由于云控有第三方云平台的支持，维护成本通常比较低，仅需要 1 个普通工作人员维护即可。但由于云平台通常采用的是猫池厂商以及打码平台的工具，且账号通常提供给多个用户共同使用，防止平台封 IP 号能力较差。

图 28：精控、群控、云控

图：精控

图：群控

图：云控

数据来源：百融行研中心

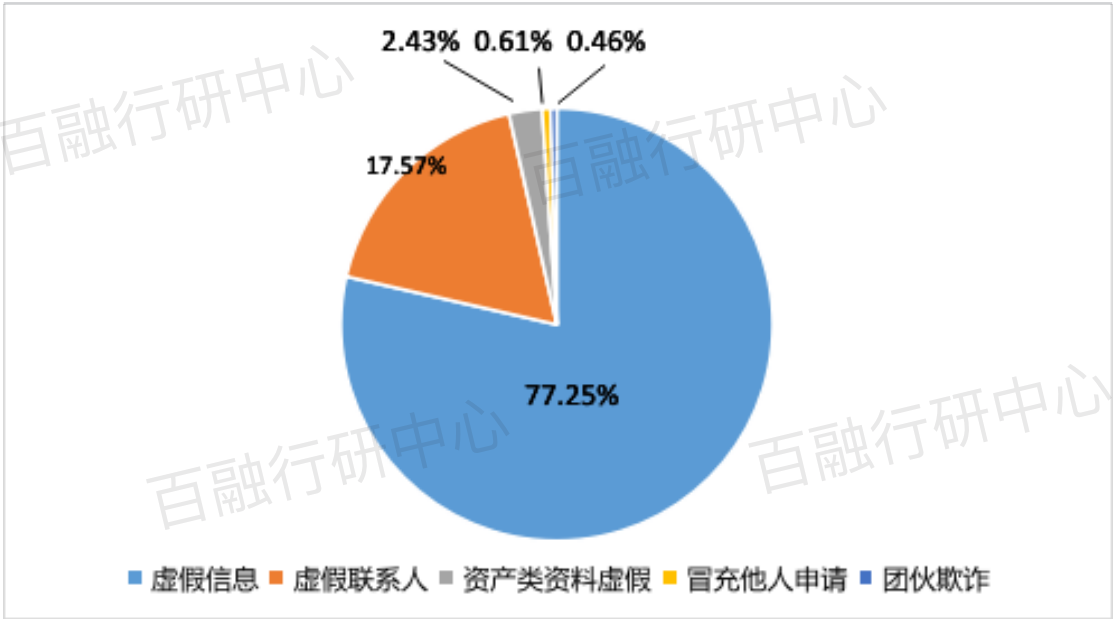
羊毛党对于平台的攻击，一般只限于营销、注册以及登录环节。由于羊毛党攻击金融机构使用的手机卡大多是虚拟卡以及没有经过实名验证的手机卡，金融机构针对线上申请的信贷业务，可以设置规则禁止虚拟卡的申请，并通过运营商 3 要素验证申请人姓名、身份证、手机或者通过银联 4 要素将银行卡同时进行核验，一定程度上可防止羊毛党对信贷申请环节的线上批量攻击。但运营商、银联的 3、4 要素验证，通常收费较高，面对批量的攻击容易提升金融机构的运营成本，金融机构可以采用设备指纹技术 + 虚拟卡拒绝规则前置的方式在耗费最低的成本同时拒绝掉尽可能多的羊毛党以及信贷欺诈客户。

03 信贷欺诈

三、信贷欺诈

信贷欺诈是指通过资料盗用、包装的方法，骗取银行贷款的行为。按P2P行业的主要信贷欺诈行为进行统计，截止至2018年第三季度，信贷欺诈风险比例最高的欺诈行为分别是：虚假信息（占比77.25%）、虚假联系人（占比17.57%）、资产类资料虚假（占比2.43%）、冒充他人申请（占比0.61%）、团伙骗贷（占比0.46%）。

图29：P2P行业5种主要信贷欺诈行为



数据来源：易观方正证券研究所，数据整理：百融行研中心

3.1 信贷欺诈类型

3.1.1 工作信息欺诈

在5类主要信贷欺诈行为中，信息虚假（例如职业、工作等相关联系信息）占信贷欺诈比例的77%左右，其中涉及申请人工作信息欺诈的情况较多。另外中介代办包装当中也包含单位资料包装的风险。其主要原因是工作收入是申请人的第一还款来源，直接影响金融机构对申请人的资信评估。好的工作单位意味着申请人工作更稳定，收入水平更高，还款能力更强；且工作单位固定电话能够作为还款提醒、逾期催收的有效手段，能有效提高申请人违约成本，从而控制风险。如果单位资料包装的风险在贷前审核的过程中未能发现，贷后容易出现失联的情况；同时金融机构对不同客户群体的信用评估也会受到影响出现偏差。

申请人的单位资料包含单位名称、地址、固定电话三个常用信息，单位资料信息欺诈，主要包括以下类型：

◆ 职业信息虚假欺诈行为，主要包括：（1）申请表单位虚构；（2）申请表单位真实存在，但申请人非申请表单位员工等。

◆ 代办包装欺诈行为，主要包括：（1）申请表单位为信贷中介；（2）申请表单位真实，但单位电话为中介电话；(3) 申请人通过缴交社保公积金的方式挂靠申请表单位。

◆ 工作相关联系信息虚假，主要包括：（1）申请表单位信息真实，但固定电话虚假；（2）申请表单位信息真实，但单位地址虚假；（3）申请表单位信息真实，但单位联系人虚假。

3.1.2 虚假联系人

虚假联系人占信贷欺诈风险的比例为 17.57%，主要细分成以下三种情况：（1）虚构联系人；（2）联系人身份虚假；（3）联系人为申请人本人。

由于部分网贷平台无需提供借款申请人单位信息，仅需要提供本人的亲属、同事、朋友作为联系人信息。当申请人出现逾期时，除了对申请人催收以外，只能够通过跟联系人沟通对申请人施压，如果联系人信息虚假，则无法达到预期的催收效果。

由于联系人的伪装比工作单位更加容易，联系人一般仅提供姓名、手机，且这些信息无法进行实名校验，在风控审核环节一般很难发现该类风险。银行信用卡的网申渠道以及通过 APP 申请的信贷产品可以要求申请人在手机通讯录中选取联系人，但部分欺诈分子会在申请信用卡、信贷产品前伪造通讯录，以混淆金融机构的视线，完成虚假联系人资料的包装。

3.1.3 资产类资料虚假

资产类资料虚假，多见于抵押贷款以及需要提供财力资料的信用贷产品中。申请人通过伪造资产资料骗取金融机构的贷款或者提升授信额度，最常见的资产资料虚假有：（1）房产证虚假；（2）行驶证虚假。

目前国内各地区的房产证没有统一的格式，一般通过封皮、用纸、团花、水印、签发机关盖章等辨伪点进行识别，或者到当地房管局管理网站通过编号进行查询。对于需要线下面签的信贷产品尤其是房抵贷这类需要进行房源尽调的产品，伪造的房产证识别起来比较容易；对于线上进件的信贷产品以及依托无纸化系统进行集中审批的金融机构，由于风控审核人员无法接触到原件，如果欺诈分子获得了真实房产证的编号，则金融机构无法确定房产证的真伪。且单纯依靠人工辨伪，无法实现自动化审批。

图 30：真假房产证

数据来源：网络公开数据，数据整理：百融行研中心

2004 年以后，行驶证由公安机关交通管理部门实行全国统一发放，行驶证相片、底板、印章、印刷字体都有明显的防伪标示，可以通过防伪点或者第三方行驶证数据进行真伪验证。目前市面上有将行驶证防伪点跟 OCR 结合的方式，能够自动识别伪冒行驶证，提升自动处理效率。

3.1.4 冒充他人申请

冒充他人申请，主要分为本人知情与本人不知情两类。本人知情的情况又称为白马欺诈，是指本人允许别人用自己的名义和信用记录等信息申请贷款的行为。白马欺诈主要有两种情况：（1）资信较好的用户（名义申请人）利用自己的资料为无法获得金融机构授信的用户（实际申请人）获得贷款、信用卡等服务；（2）欺诈分子通过返利、承诺无需还款或部分还款等方式，诱骗其它用户提供资料帮其申请贷款；

情况（1）中，由于名义申请人信用较好、还款能力较强，如果实际申请人出现无法偿还的情况，名义申请人代为还款的可能性较大。且由于信用卡以及现金分期产品没有明确的资金用途，难以对名义申请人以及实际申请人进行区分，所以被金融机构核查出风险的概率较低。

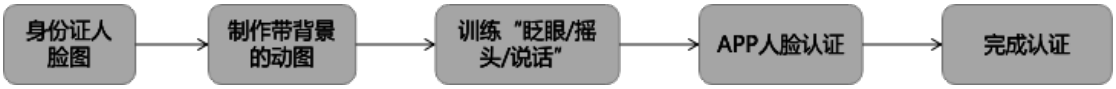
情况（2）中，欺诈分子主要通过两种方式获取名义申请人资料。第一种方式是打着远低于市场价格购买 3C 产品或教育、旅游、医美等服务吸引用户提交资料办理信用卡或者消费分期。第二种方式是欺诈分子针对农村留守人员、娱乐场所员工、无稳定工作的自由职业者或者有黄赌毒不良嗜好的群体，通过许诺返回一定的利益的方式或者威吓、强制扣留身份证的手段获得名义申请人资料。这种类型的名义申请人，通常有强烈的资金需求且征信、安全意识淡薄，一旦金融机构发放贷款，回款的概率极低。

在本人不知情的冒用案件中，欺诈分子通过黑、灰产购买用户的身份证、手机号以及银行卡信息，并伪造身份证申请信用卡、贷款。由于身份证有较为明显的防伪标识，一般的伪冒身份证通过人工排查很容易分辨，

但处理效率较低，金融机构可以尝试防伪点与 OCR 相结合的方式，提升自动化处理比例与效率。部分欺诈分子通过黑产购买到用户遗失的身份证，通过该证件进行申请信用卡、贷款，金融机构可以通过活体验证以及人脸比对的方式对申请人的身份信息进行校验，排除欺诈风险。另外，金融机构一般会保留存量客户的身份证信息，部分金融机构在存量客户进行二次申请信贷业务的时候，无需对身份证信息进行校验，欺诈分子一旦得到了存量的身份信息，很容易就能够通过金融机构的风控，骗取贷款。

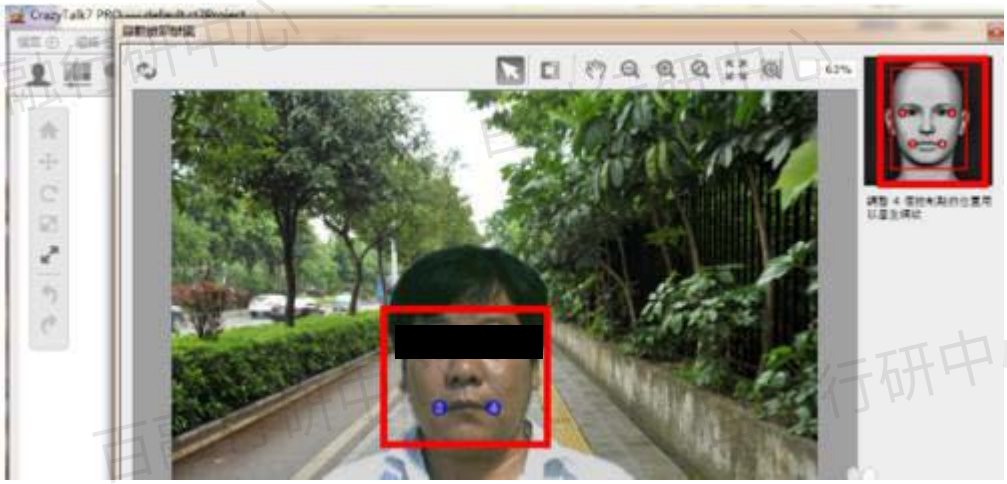
目前针对线上进件的机构，黑产已有破解人脸识别的技术。黑产获得身份证原件或照片后，通过电脑制作带背景的动图，并且合成制作眨眼、摇头、说话、张嘴等动作，从而通过平台的人脸识别，达到冒用身份的目的。

图 31：人脸识别破解流程



数据来源：百融行研中心

图 32：人脸识别破解示例



数据来源：百融行研中心

3.1.5 团伙骗贷

（1）什么是团伙骗贷

团伙骗贷，是指欺诈分子有组织、有计划的对一家或多家金融机构实行贷款诈骗的行为。团伙骗贷通常表现为同一批申请人申请时间、地点接近，工作单位、工作岗位相似，资产资料有较为明显的共通点。通常由一

名或者多名欺诈分子对金融机构进行试探性申请，一旦通过申请后，欺诈团伙就会按照这名同伙的资料为其它申请人进行包装，并总结金融机构的风控政策与审核规律，使之后的申请更容易获得金融机构通过。

（2）团伙骗贷的特点

团伙骗贷的金额通常较大，一般倾向选择银行大额现金分期产品。欺诈团伙挑选征信白户或者征信记录满一年但信贷记录不多的群体，并对其资料进行包装。为了伪装资料，使申请人的信息尽量真实以便通过后续审核，同时降低被金融机构进行反欺诈调查的可能性，欺诈团伙一般都只挑选本地的申请人进行包装。大型的欺诈团伙通常有明确的分工：第一组负责寻找合适的申请人；第二组通过黑产购买用户信息、虚假证件、资料并进行包装；第三组专门研究金融机构的风控策略，并负责电话审核的应答。另外由于团伙欺诈金额较大，通常伴随着内外勾结行为，其中银行的客户经理、非银行金融机构的业务员以及驻当地的风控人员，更容易受到当地黑产的诱惑，为其提供金融机构的内部信息。

3.2 信贷欺诈手段

信贷欺诈的手段主要包括：申请人固话转接、固话代接、中介包装、养卡养号、内外勾结五种。

3.2.1 固话转接

在申请信贷业务时，金融机构看重申请人的工作性质、收入以及稳定性，部分资信或者工作单位一般的申请人，为了获得银行授信，常将机关单位、事业单位、知名大型企业作为申请工作单位，并将自己的单位、家庭固话伪装成优质单位的工作电话，自己接听金融机构的核实电话，伪装成在优质单位上班，误导金融机构电话审核人员。部分申请人由于经常需要外出，会将固定电话设置成来电转接状态，拨打该固定电话将自动转接到申请人手机上，在固定电话中输入“57”＋需要转移的电话号码，即可实现无条件呼叫转移（如图 33）。

图 33：固定电话转移

数据来源：百融行研中心

在淘宝中搜索“固话转接”可以找到一批专门提供固定电话服务的电商，该类电商主要提供固定电话转接与固定电话代接的服务。

选择固定电话转接服务，电商提供一个用户指定地区的固定电话号码，且在一定时间内拨打该号码，会转接到用户指定的手机上。其原理跟用户自行设置固定电话转接类似，但无需申请人自己准备固定电话，且能伪装其它城市的工作固定电话，更适合没有办公、家庭固定电话的申请人以及跨地区开展业务的欺诈分子。

电商提供用户呼叫转移的固定电话号码一般是虚拟电话，虚拟电话即网络电话，也称“一号通”，是按照信息产业部新的《电信业务分类目录》，具有真正意义的 IP 电话。集通话、传真、留言、电子邮件、短信、呼叫转移、自动寻呼、密码保护等多项功能于一体，永不占线且可移动。它比传统的“呼叫转移”功能强大和完善，是一项电信业务。

虚拟电话克服了传统电话功能单一，只能接、打电话的缺点。相当于传统的“小总机”，它的核心是一个多通路、可以终生使用的个人通信电话号码，具有“三打三通”的基本功能。将三个电话号码（本地或外地甚至国外的小灵通、固定电话、手机等）输入到虚拟电话中，虚拟电话即能按照用户的要求将来电转移到用户指定的多个号码上。遇占线或无人接听，来话将自动按用户事先指定顺序转移到所设置的其他号码上，直至找到用户本人为止。虚拟电话可以通过网上进行设置，包括功能设置和修改要转接的号码等，修改是用户自助的，且即时生效。

一般的电商仅能提供国内几个城市的虚拟电话，但是一些大型的虚拟电话运营商，如傲天信息科技、新航通等，除了能够提供国内各个城市的虚拟固定电话外，还能够提供全球各个国家的虚拟固定电话号码。

图 34：虚拟固话覆盖地区样例

数据来源：网络公开数据，数据整理：百融行研中心

在傲天信息科技开通虚拟电话，一般需要交 300 元的预付费，接听及拨打 0.3 元 / 分钟，不同的城市有不同的预付费收费标准。

图 35：虚拟固话收费标准样例

数据来源：网络公开数据，数据整理：百融行研中心

3.2.2 固话代接

在淘宝中搜索“固话代接”可以找到一批专门提供固定电话服务的电商，该类电商主要提供虚拟固定电话代接的服务。

办理固话代接业务，电商通常先跟申请人确认需要哪个城市的固话以及固话用途，大致上可以分成（1）办理信用卡；（2）办理贷款；（3）签证；（4）入职调查，共四种。然后电商再跟申请人确认单位信息由电商提供还是申请人自行提供，若选择由电商提供单位信息，对方会提供公司名称、地址、电话及其他一些基本信息，申请人提供个人基本信息给电商后可以通过该公司资料进行信贷或者其它业务的申请；若选择申请人自行提供单位资料，则需要提供申请人提供姓名、手机号、性别、年龄、职位、收入、单位名称、单位地址、公司法人、公司主营业务信息等。

图 36：固话代接

数据来源：网络公开数据，数据整理：百融行研中心

固话代接一般按可分为 7 天、15 天、30 天代接，根据代接的时间长短收取约 50-150 元不等的费用，服务期间代接固定电话不限次数。

电商提供固话代接服务时，由于对客户申请贷款产品、金融机构的风控政策不了解，且需要同时应对较多申请人的电话应答，代接容易出现应答错误，且固话代接通常一个月的费用只需要 150 元以内，对于代接电话的电商而言，信用卡、贷款是否批核成功对其利润没有影响，故通过电话代接的方式包装资料，被金融机构的电核人员发现欺诈风险的概率较高，不但无法获得贷款，更容易被银行标记为欺诈客户从而失去授信的机会。

3.2.3 中介包装

行业内存在着一批专门替申请人包装资料获取金融机构贷款并从中获利的群体，称为信贷中介。由于信贷中介对金融机构的产品熟悉，且部分中介是风控转行而来，对各家平台的风控政策有研究，能够根据申请人的具体情况选择更容易通过审核的平台。与电话代接相同，中介在包装申请人单位资料的时候，一般会选择虚拟

电话，因为可以对接全国各地的业务。但有部分中介只接受本地的申请，因为中介对本地的企业情况更为熟悉，容易应答电话审核员提出的问题，且部分中介在本地金融机构中有同伙，能够使中介的申请更容易获得通过。除此之外，部分中介还能为申请人提供资产资料的包装，包括驾驶证、房产证、工资流水等，从而获得金融机构更高的授信额度。中介包装申请贷款，通过率比自行包装以及固话代接高，容易吸引一些资信较差的申请人以及无稳定职业的征信白户前来申请业务。

图 37：各类资料包装方式的利弊

欺诈方式	固话转接	固话代接	中介包装
费用	约 20-50 元	约 50-150 元	贷款余额的 15%-50%
时间	无限制	7 天、15 天、30 天	申请贷款到放款
下款概率	较低	较低	较高

数据来源：网络公开数据，数据整理：百融行研中心

由于中介在金融机构放款后通常会收取申请人放款金额 15%-50% 的费用，容易导致原本资信不佳，还款能力弱的申请人失去还款的意愿。且通过包装的工作单位固定电话并不能在放款后联系上申请人，一旦申请人手机发生变动，很容易出现失联的情况。

3.2.4 养卡

所谓“养卡”，就是“养卡”公司先用自己的现金替持卡人将欠款还上，让信用卡显示正常还款，随后再通过刷 POS 机等虚假消费的方式把卡上相应额度的现金套出来，以维持持卡人正常的信用记录，不会产生逾期利息。

部分欺诈分子在通过资料包装获得银行等金融机构授信后，不会直接将信用卡或者金融账户中的资金取出来，而是会用这张信用卡正常消费一段时间，甚至办理一些消费分期业务，待银行提升其授信额度后，再将资金套现出来。与此同时，欺诈分子还会利用申请该信用卡的资料申请其它银行的信用卡以及信贷产品，由于银行在新发信用卡时通常会参考其它银行信用卡的用卡、还款记录，所以经过养卡的欺诈分子更容易获得其它银行的授信。待欺诈分子认为银行授信额度足够多时，就会将所有信用卡的额度一次性套出，然后失联，给金融机构造成大范围的损失。

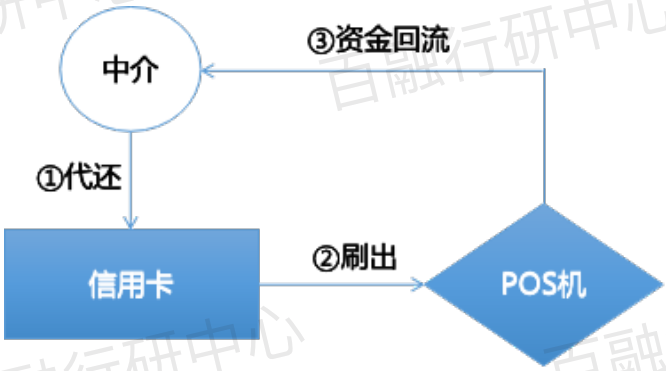
从历史发展来看，养卡有三个发展阶段，每个发展阶段对应有三种不同养卡类型：

图 38：三种养卡方式

数据来源：百融行研中心

在养卡黑产出现初期，各个中介主要采用代还的方式提供服务，比如信用卡持有人还款日到期了，代还中介直接代还相关金额到持卡人账户里进行还款，然后再把相关金额刷出来，以此来达到养卡的目的（如图 39）。

图 39：信用卡代还流程



数据来源：百融行研中心

此服务兴起是因为成本较低（最低能到几十块一笔），利润相对较高（一笔服务费 2% 起）且容易达到规模效应，同时如果持卡人想要通过其他渠道进行借款还债，比如小额贷款，所需花费的成本相比信用卡代还要高得多且时效性差。所以该中介服务得到了快速发展，市场需求火爆。

第二个阶段为代刷代还阶段，只需要持卡人直接提供信用卡到中介处，约定每月刷卡频率和金额后中介会定期按照约定频率进行刷卡和代还服务，待刷信用卡提额至最终目标额度时，再返还给持卡人（如图 40）。

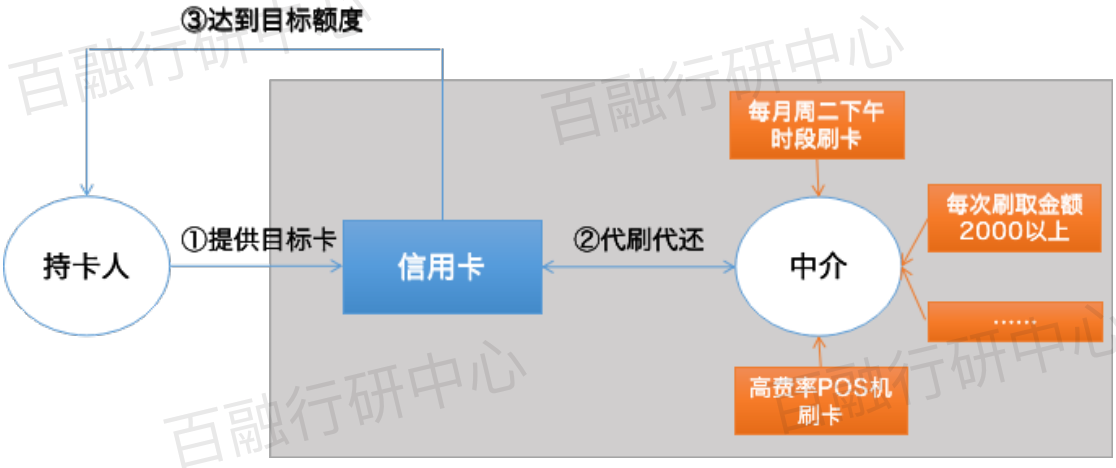
图 40：信用卡代刷代还流程

数据来源：百融行研中心

这种养卡方式对于双方来说都各有好处，对于持卡人可以不用每期找刷卡和代还中介，对于中介来说可以批量操作 ,同时可以在各个卡内部进行现金流操作(比如用 A 卡刷出的钱还 B 卡的账)以此节约一定现金流成本，并可扩大经营规模。

第三个养卡阶段也就是目前市场上经常出现的精养卡。所谓精养卡也就是每家银行对于信用卡提额的触发点各有异同，中介通过不同目标银行对于信用卡在每月刷取额度、商户费率以及刷卡时间等评判维度的不同要求，对目标卡进行精准刷卡代还的活动，以达到更加快速高效达到目标额度的养卡方式（如图 41）。

图 41：信用卡精养卡流程

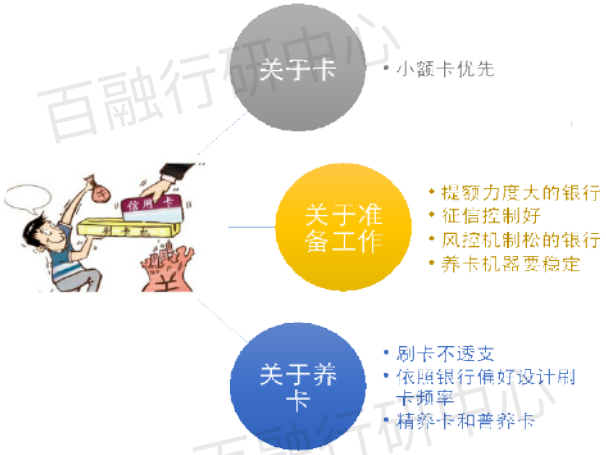


数据来源：百融行研中心

此种方式对比代还代刷的方式养卡速度更快，某些情况下 3 个月即可完成提额，慢的可能需要半年时间，并且中介还可同时收取代刷代还手续费。

从养卡行业的养卡偏好来看，中介突破的方面有以下八个维度：

图 42：中介养卡八个关注点



数据来源：百融行研中心

（1）首先从被养的信用卡出发，中介更偏好小额度卡片，因为卡片本身额度越小代表未来能提额的空间越大，对于中介能赚取的手续费也越可观。但这跟本身提额银行的政策和卡的特性也有关系，有的银行的某类特定信用卡（比如缴费类）提额空间本身就有限。

（2）从前期准备工作来看，中介会网罗提额力度大的银行进行特定养卡，同时有些中介还会同时关注银行的信贷政策，因为有些银行信用卡提额难，但是信贷较为宽松，那么转为养贷也是可以的；

（3）中介还会提醒持卡人注意征信表现，比如注意总负债情况、总卡数情况、负债率以及贷后管理次数等等，避免后期影响提额；

（4）对于银行的风控政策，中介也会多多关注。如果银行的风控政策较严格，例如中国交通银行，中信银行，平安银行，中国工商银行，浦发银行以及中国招商银行等，这些银行对提额要求比较严格，对于刷卡时间、刷卡商家以及刷卡额度都会有较严格限制，不能轻易提额；

（5）对于养卡器而言，比如 POS 机，长期运营的中介会选择稳定且品牌有保障的供应商，而对于短期的中介机构而言，不正规（比如刷卡利率异常低、免费送机器或者不明品牌等）的机器进行养卡，而此类时常出现的刷卡金额较正常养卡刷出的金额大。

（6）对于养卡方式来说，中介会尽量不进行透支，会预留额度的 10%-20%，最低不会低于 5%，以避免遭到封卡或者冻结，后续操作会比较麻烦；

（7）中介会依据银行偏好进行刷卡，比如某银行现阶段鼓励用户在 APP 端进行刷卡且双倍积分，那么就要多使用手机端进行刷卡，再比如刷卡金额和频次要符合提供的基本信息的逻辑，如普通工薪阶层，购买的物

品件均和档次银行都是有预判的，刷卡金额不能过于离谱；

（8）最后就是总的养卡方式，是采取精养卡还是普养卡，这个要依据持卡人偏好，一般精养卡刷卡频率每月在 20 次以上，普养卡在 10-15 次以上。

从养卡中介利润来看，还是比较可观的，一般养卡中介收入来自以下几个方面：

图 43：养卡中介收入来源

数据来源：百融行研中心

通过粗略的测算，假设某养卡中介每月养卡 1,000 张，平均每张额度 10,000 元，市面上一般精养卡收费为 1 万元额度收取 150 元 -300 元不等的手续费，成本大约在每张 55 元 -60 元不等，此时按照最低收入 150 元和最高成本 60 元来计算，该中介每月养卡手续费收入最低 =1,000*（150-60）=90,000 元；同时批量养卡一般是机养（即 POS 机刷卡为主）。手养（非机器刷卡，手动代刷代还）一般涉及套现较多，且养卡中介在 POS 刷卡时还可以从 POS 机代理商处分得一定的刷卡手续费，一般 10,000 元刷卡金额会给中介分得 2-3 元手续费，按照最低额计算，该养卡中介每月可得 2,000 元手续费收入；并且对于持卡人的每月刷卡积分，一般都会约定最后为中介所有，而这部分积分中介可通过其他中介机构进行积分套现，1,000 万元的总量平均每月能有 100 万左右积分，折算现金可得 1,500 元左右；最后是收取持卡人的提额费用，前面有介绍过，对于养卡中介，养卡费用和提额费用是分开收取的，这里假设精养卡 3 个月，1,000 万元提额 10%，总提额 100 万元，提额费用这里按照 8% 计算为 8 万元（一般养卡收费为 8%-15%），月均 2.67 万。最终该养卡中介每月利润所得为 90,000+2,000+1,500+26,700 ≈ 12 万元。

再来看成本，养卡中介的成本一般很低，包括了四个方面：人工（5 名以内员工）、办公场地（小型办公场地即可）、POS 机费用（可租用也可购买，一般 50 台 POS 机月均成本 1,000-2,000 元不等）以及相关养

卡软件费用（月均几百到几千元不等），总共算下来一个小型养卡机构月均成本能控制在 2 万元以内，净利润算下来能达到 10 万元。

3.2.5 内外勾结

内外勾结，是指金融机构内部人员与外部中介、欺诈团伙串通，将公司内部的风控政策、策略甚至申请人资料提供给不法份子，帮助其进行资料包装并骗取金融机构授信的行为。

金融机构从业人员内外勾结，主要有三种途径。

（1）透露客户信息

第一类是单纯透露客户信息以谋取私利，对机构会造成很坏的社会影响。

单纯信息泄露是指在借款人本人不知晓的情况下，内部人员对借款人信息进行泄露，联合中介机构以达到获利的目的。

从银行案例来看内部人员泄露信息最高发的风险行为当属偷查个人征信报告：

案例 1：银行职员 A 利用职务之便，盗取同事银行征信系统用户账号和密码，再找寻相关买家（多为民间借贷机构）后，通过买家提供的公民身份信息，利用盗取的征信系统查询权限提取相关人行征信报告，并以每份 10 元价格提交给买家进行牟利，三个月时间内职员 A 共提供了 9,000 多份个人征信报告，非法获利 9 万余元。

数据来源：百融行研中心

案例 2：2016 年某地媒体曝光出大规模个人征信倒卖案件，当地警方抓获相关人员 15 名，查获个人征信信息 257 万条，涉案资金达 230 万元。此案中，某银行县支行行长 B 和中间商机构 C 通过互联网方式，将账号租用给 C，并根据查询量进行提成，而 C 再通过查询结果和其他 DEF 等中介机构（比如小贷公司、金融服务机构等）达成合作关系，批量出售个人征信报告。

数据来源：百融行研中心

第二类是直接在借款人知情的情况下，内部人员和中介机构联合利用泄露信息薅羊毛。从非银案例来看内部人员泄露信息最常见的为黑名单类客户包装：

案例 3：欺诈团伙在金融机构的内应，会将金融机构被拒绝的申请人资料以及拒绝原因提供给欺诈分子，并告知其如何对申请人进行资料包装（例如禁入行业改为非禁入行业、收入档次不够、本人命中硬性黑名单换位亲属来申请等）。然后由中介负责跟被金融机构拒绝的申请人联系，称可以帮助其重新获得银行的授信，从而吸引部分资金饥渴的申请人在中介办理业务。办理成功以后，中介会给金融机构内应人员分成。

数据来源：百融行研中心

（2）协助审批中介包装进件

相比直接透露客户信息，还有一种内外勾结不用顺应相关政策去想方设法绕过不符合借款的雷区而达到最终目的，那就是直接提供虚假信息或者直接进行批核，从而在操作环节降低对经过中介包装申请的审批要求，进而通过审核获得授信。

第一类，直接提供虚假信息。

数据来源：百融行研中心

案例 4：大庆男子 A 在明知自己没有还款能力的情况下，通过银行机构内相关朋友指引，与银行签订了信用卡汽车专项分期付款业务合同。在签订过程中，通过中介和机构内朋友包装，提供了虚假房产证和收入证明，骗取了某融资担保公司提供的担保，取得银行购车款近 20 万元，最终由于前几期一直未还款，银行诉讼至法院，经裁决相关人员构成合同诈骗罪，被判入狱。

第二类，内部操作风险，相关审核人员对不符合资质的申请人直接批复通过。

案例 5：2015 年，一家国有银行的支行被广州两家空壳皮包公司先后诈骗共计 2,600 万元，时任某国有银行支行的信贷员李某在经办该公司贷款业务中，未按规定严格执行实地调查核实贷款资质，整个贷前调查流于形式，贷后也未严格监管。而身为小企业金融部经理的邝某、主管信贷业务的副行长陈某也在未深入调查的前提下批核了该笔借款，导致该公司诈骗成功，形成不良贷款。究其原因，是因为领导介绍而导致整体调查流于形式所致。

数据来源：百融行研中心

（3）泄露金融机构风控政策

欺诈分子在金融机构的内应，如果是能够接触到风险以及审批政策的岗位，可以直接将风险、审批政策透露给黑中介，黑中介根据提供的信息寻找合适的申请人，并通过资料包装的方式顺利通过金融机构的风控。在前文提到的中介现状当中，部分中介就是通过这种方式来发现风控口子的。

中介会跟金融机构的风控人员进行接触，请风控人员协助其进行内外勾结，并承诺给与风控人员一定的报酬。由于一般风控人员通常都是领取固定收入，较容易受到外界利益的诱惑。部分中介甚至会要求风控人员提供其它同事的联系方式，然后再通过短信、电话的方式与其接触。提供同事通讯录的内应也会视情况进行穿针引线，让更多的风控人员参与内外勾结。个别金融机构，甚至连负责反欺诈调查的部分负责人，也是内外勾结的参与者之一。

案例 6：某知名 P2P 关联的放贷端的烟台分公司某员工联合总部风控人员、分公司客服人员，利用自身熟悉风控规则体系以及整体审批放贷流程，在各县市区拉了 72 名借款客户，并联合中介为所有借款人做假银行流水及社保证明以满足公司进件要求，据统计，共向总公司借款 600 余万元，借款额中的 10%-20% 给了借款人，剩下的借款除了履行前六期还款以外，全部被案件嫌疑人侵吞。

数据来源：百融行研中心

从以上内外勾结形式来看，最核心的就是员工道德风险，其涉及的手段的维度主要有利用虚假信息进行包装、绕过或者刻意符合进件资质（比如刷流水、本人不符转由亲属借款等）、风控失职（例如不严格执行风控审批流程，直接批核等）以及泄露客户信息或者公司政策等。因此，为防止内外勾结，人员管理是核心，所以需要金融机构完善相关的内控机制，严控操作风险。

（1）加强管理体系建设

图 44：管理体系建设

数据来源：百融行研中心

管理模块化

对于风控部门，不同岗位设置不同的权限，仅能够了解岗位权限内的信息。若需要了解其它岗位、部门的信息，需要由直属领导进行批示。例如分公司审批或者风控人员不参与决策，只对搜集信息负有客观性责任，审批应集中交给总部处理。再例如某部分自动化审批模块不再交由人工审批，或者人工审批只能在规定范围内进行决策，以控制操作风险。

管理整体化

风险管理体系应建立相关机制，各部门之间相互协调、相互配合，共同运作风险管理机制，整个机构是一个有机整体。从申请人进件到审批放款，每个环节应有不同岗位进行负责，且只有特定岗位才有特定权限，但是同时这些模块要组合在一起才能最终出结果，以此来降低某些岗位裁定的权重。

管理纵深化

某部分核心人员由专职团队统一管理，比如相关流程、相关指标以及相关动向，都应及时报备和征求专家意见，以此来降低团伙欺诈的风险。

管理制约化

管理制度和业务流程相互制约，风险管理体系应按照相互制约（即业务流程与部门设置既要考虑各个环节的制衡关系与风险控制，又要有利于工作效率提高）的原则来设置业务流程及内部控制机制。比如业务的绩效指标和风控的绩效指标要相互挂钩以进行制约防止留下相互勾结的漏洞。

管理定制化

风险管理体系的设计应结合积累分析的自身风险特点、公司的经营规模以及当前的宏观经济环境，使风险管理体系 “因地制宜、因时制宜”，以达到风险控制与管理的目的。

（2）完善信息安全及反馈制度

内部信息安全管理

对于开会讨论的信息，会后及时进行清除。内部沟通，以信息最小化及必要化为原则，不传递必要沟通内容以外的信息。

及时反馈

风险管理体系应运用信息管理手段进行科学管理，通过信息管理系统建立风险预警系统并及时反馈、协调、完善和纠正，以达到风险控制的目的。

（3）设立内控部门或者流程

设立内控部门

除了通过特殊的方法调查欺诈案件，更专门调查内部员工是否存在操作失当以及内外勾结的情况。比如以属地管理为主导、专业部门直管、其它部门协管相结合。定期对整体业务流程或者相关人员开展专业考评、业务培训、风险指引和案件防范等工作。

定期宣导

信贷机构应加强对信贷人员的培训，培训内容除包括业务知识、法律知识、信贷技术等之外，还应加强对信贷人员德育方面的培训。在上面多起案例中都出现了员工失职、内外勾结等情形，信贷机构除了需要通过制度约束业务人员不要犯错误之外，还要通过培训、宣讲等形式加强对业务人员的德育教育，本着预防的目的，须与业务人员讲清楚尽职免责的内涵以及未尽责将面临的严重后果。通过集中学习、专题培训及个人自学相结合等方式，组织客户经理对应专业岗位，开展重要制度学习，加深对规章制度的理解和把握。引导客户经理树立正确的价值观，自觉养成诚信守法的职业素养。

（4）提升核心人员素质

提升队伍整体素质

从招聘开始，要对相关人员的职业道德、金融基础理论、银行产品知识、基本业务技能、服务及营销技巧

等方面都进行严格把关。例如有些金融机构入职是要求查询个人征信的，对于有污点的人员不予录取。同时队伍建设也应放在更加突出的位置，既要保护好，更要管理好。从源头把控队伍整体素质。

完善人员选聘机制

通过内部选拔减少了沟通成本和培训成本，同时可达到优化整体人员配置的功能，因为面对激烈竞争，内部人员的能力和适合岗位会得到一定的优化。同时也可通过对外招聘保持或者提升内部竞争水平。

3.3 关键参与者 - 信贷中介解析

前面我们提到，信贷中介是专门替申请人包装资料，获取金融机构贷款的公司。他们服务的主要客户为信贷黑户。信贷黑户是指有不良征信记录或者较严重信贷逾期记录的群体，这类群体基本无法在银行获得贷款或者办理信用卡。黑户是贷款申请欺诈的主要参与者，除此以外还有无稳定收入或者高负债人群。信贷中介主要通过寻找各类信贷平台的风控漏洞，帮助黑户以及其它两类高危群体进行资料包装，以获得信贷平台的授信，并从授信额度中，抽取 15%-50% 不等的回扣作为收入。

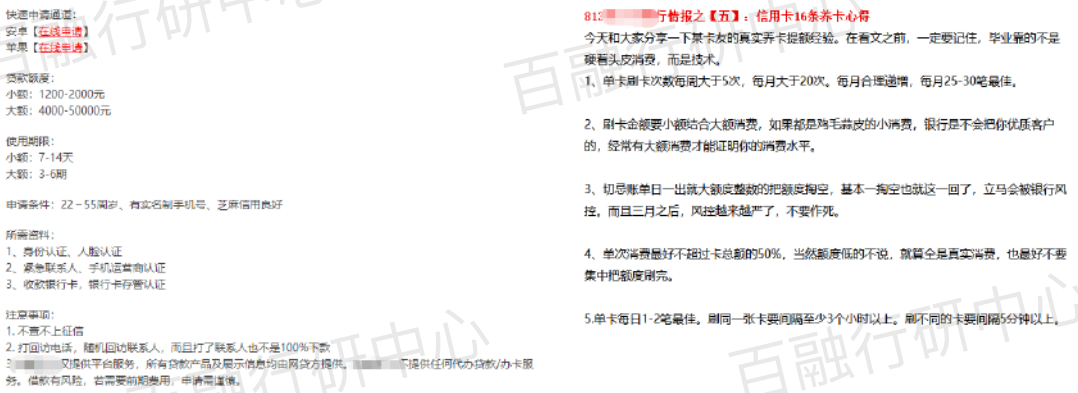
信贷中介帮助黑户获得贷款后，对已经有欠款记录的黑户来说，新增一笔欠款的违约成本会低于一般的申请人，且需要承担高额的回扣，容易导致黑户继续发生欠款逾期行为。除黑户外，无稳定职业或高负债人群通过中介包装获得贷款，同样会产生过度授信及资金链断裂的风险。

中介常说的“口子”,就是我们平时说的风控漏洞。由于网贷平台通常在 APP 上可完成申请 ,具有申请便捷、审核快、放款快等优点，适合短期资金周转不开的人群。且网贷平台通常无需面签，资料盗用、包装难度相对于线下业务容易。所以成为中介主要攻击的对象，中介们通过分享这类风控漏洞，吸引更多有资金需求却无法获得授信的高危客户群体前来办理业务。

在一个行业内知名的信贷网站中 ,各种类型的讨论帖如：“信贷套路“、”办卡提额攻略“、”黑户贷款“、”贷款破解技术“等，平均每天有 10 个以上的新“口子”在论坛中通过帖子公布，每个产品都列明额度、利率、期限，入组条件、适合人群、所需资料、审核要点等信息，并为访客提供了不同机型的申请渠道链接，方便借款人下载 APP。这些帖子的阅读量从几千到上万不等，平台还有专门的管理员对当日公布的”口子“进行回顾总结，甚至发布试用心得。

来自全国各地的中介、黑户及各类资信不良的群体，在论坛中乐此不疲的讨论如何包装下款、办卡提额，如何应对轰炸催收等敏感话题。而参讨论的人群·，既有刚毕业的大学生，也有蓝领、个体户老板、无所事事的酒鬼、赌徒，以及潜伏在他们当中的中介、黑产团伙。

图 45：中介论坛发帖



数据来源：网络公开数据，数据整理：百融行研中心

行业中，除了普通的“口子”以外，还有被称为“多件套“的“口子”。所谓”多件套“是指经过中介、黑产不断研究平台风控规则后，将申请资料、风控规则、政策都相似的平台进行整合，帮助申请人一次性申请多笔贷款的特殊“口子”。申请人只要满足条件，再经由中介进行包装操作，通常能够在其中 70% 以上的平台获得贷款。 按照平台的数量，比较常见的有“3 件套”、“4 件套”，偶尔也有超过 10 个平台以上的。这类型的“口子”，中介通常会在 1 天之内同时申请，以避免部分平台多次申请的风控规则，使同时放款的概率增加。“多件套”口子在提升放款概率的同时，增加了申请人的负债比例，使申请人更容易出现无力偿还的现象，对金融机构造成的危害更为严重。

除了口子外，网站中通常会有专门的技术攻略论坛，指导申请人申请各类信用卡、贷款的要点，并介绍专业的破解工具，指导资信不良群体自行破解信贷平台风控。

图 46：中介广告

数据来源：网络公开数据，数据整理：百融行研中心

在该类论坛上公布的信贷攻略指引，通常都是入门级别的，目的是通过指引吸引更多的业务或者发展二级代理。真正有技术含量的操作，黑产、中介不会随便公布，通常需要收取一定的会员费或者代理费，才能提供。黑产，中介通常会以加微信群、QQ 群的方式对已缴纳会费的“会员”一对多或者一对一的指导，具体指导形式取决于收取会费的多少。

黑产、中介会对申请加入 QQ、微信群的会员进行筛选，要求会员在指定信贷网站的账号达到一定的等级，或者下载专用的信贷超市 APP，并通过账号在论坛发帖的频率、内容以及申请人手机的通讯录、通话记录、短信、常用 APP，判断申请人的资信以及信贷需求情况，防止金融机构的反欺诈调查员加入会员刺探情报。通过审核的申请人，需要缴纳 300-1,000 元不等的“会员费”才能够入群。进 QQ、微信群后，会有专门的管理员以及客服为会员介绍最新的贷款口子、破解工具以及操作流程。相比网页、论坛上的“口子”分享，在微信、QQ 群对会员的分享更有针对性、技术含量更高，是黑产、中介群赖以生存的核心。

图 47：中介交流

数据来源：网络公开数据，数据整理：百融行研中心

大多数的黑产、中介群接受全国范围的业务，但部分的黑产、中介仅接受工作所在地的业务。一方面是在当地的金融机构有内应人员提供协助，下款概率较大；另一方面能够降低金融机构的反欺诈调查员伪装申请人进行电话咨询的概率。

部分黑产、中介群在引导申请人或者信贷从业人员入群后，并不在群里讨论信贷“口子”以及破解技术，而是需要添加群主微信后才能获得相关的资料，用以降低黑产、中介群被查封的概率，同时尽可能防止核心技术外泄。部分中介，甚至会将申请人发展成为下线或者二级代理商，增加获客渠道。

图 48：中介业务咨询

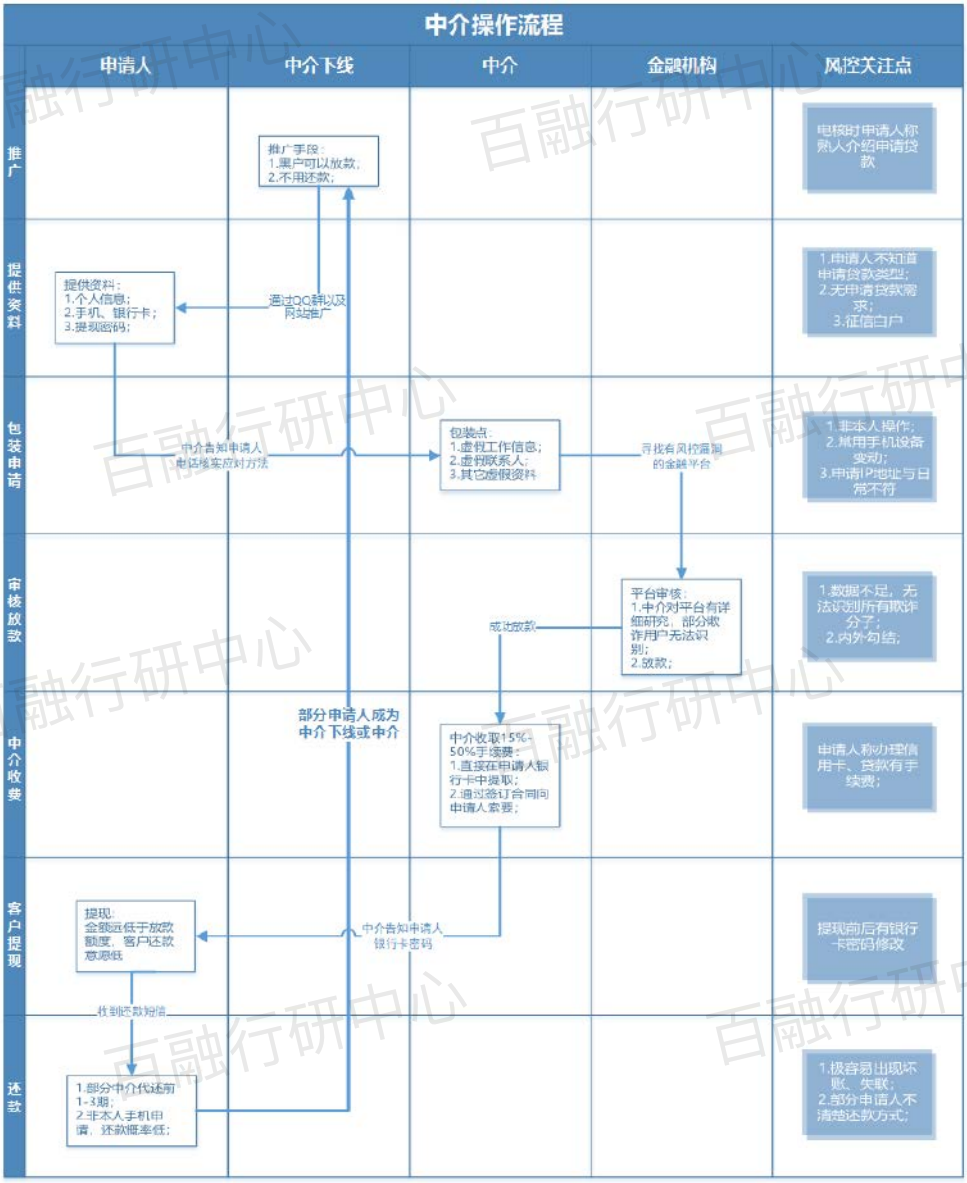
数据来源：网络公开数据，数据整理：百融行研中心

一般情况下，中介通过 QQ、微信群、中介网站广告等方式推广业务，通常中介都会宣称放款后无需还款，或者前几个月由中介代还。中介跟申请人接触后，会先与申请人商量好本次操作的手续费，通常为放款金额的 15%-50% 不等，并要求申请人提供本人姓名、手机号、身份证号、银行卡号以及提现密码等信息，并将银行卡密码进行修改，由中介进行包装并申请。平台放款后，中介先在申请人银行卡中提取操作手续费，然后修改后的银行卡密码告知申请人，由申请人将银行卡中剩余的资金取出。

由于通过中介办理业务的申请人，通常资质较差，还款能力较弱，加上中介收取高额的手续费，导致申请人还款意愿更低，更容易出现逾期坏账的现象。

部分中介在银行或者网贷平台中有自己的内应进行内外勾结，部分中介为了保护内应，通常会为申请人进行 1-5 个月的代偿，提升金融机构通过还款表现分析欺诈案件的难度。

图 49：中介操作流程



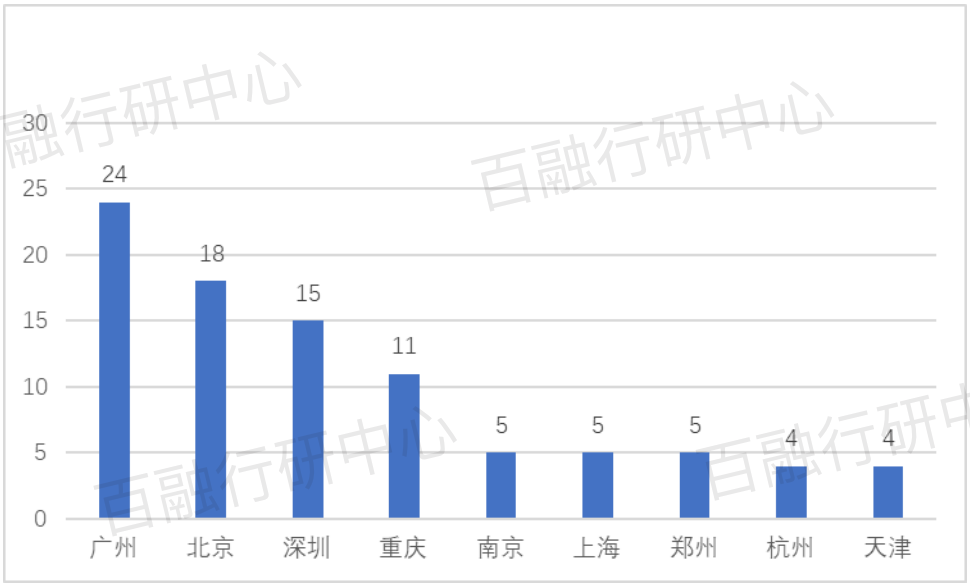
数据整理：百融行研中心

3.4 从业者画像[③]

在 QQ 的群搜索功能上输入关键字“口子”，可以搜寻出相关的 QQ 群 146 个，经过筛选去重后，有 135 个 QQ 群确定为信贷中介群且在正常运作当中。按每个 QQ 群人数进行汇总统计，信贷中介群的 QQ 成员人数超过 18 万。每个群的平均人数在 1,300 人左右。

③ 以下的从业者画像只在 QQ 群当中公开信息基础上进行分析，部分信息不可避免存在失真，仅供行业参考。

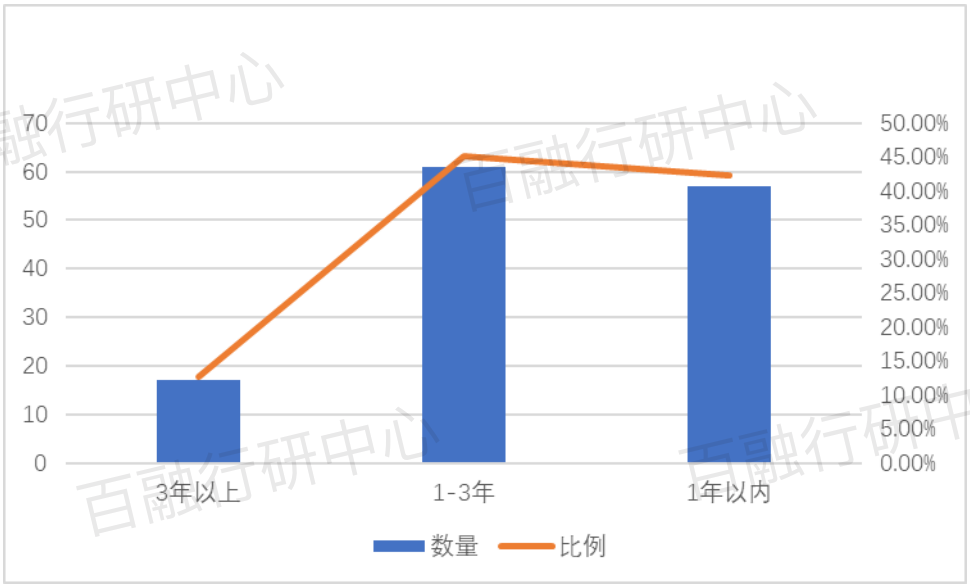
图 50：中介群发起地区统计



数据来源：百融行研中心

QQ 群根据群主的所在城市确定 QQ 群发起地点，从中介群的发起地址统计，发起地在广州的 QQ 群共 24 个，数量最多。其次是北京、深圳、重庆、南京、上海、杭州、天津等一线城市，同时电信诈骗、信贷欺诈高发地郑州也排进了前列。

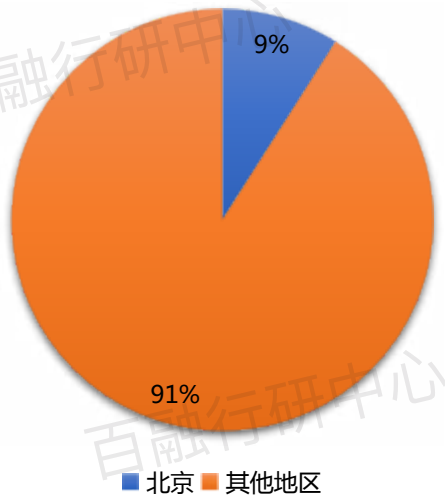
图 51：中介群成立时间统计



数据来源：百融行研中心

从中介群的成立时间统计，成立1年以内的QQ群有57个，占比42.22%；成立时间1-3年的QQ群有61个，占比45.19%；成立时间超过3年的仅有17个，占比12.59%，可以看出，信贷中介业务在2015年后伴随互联网金融的高速增长发展迅速。

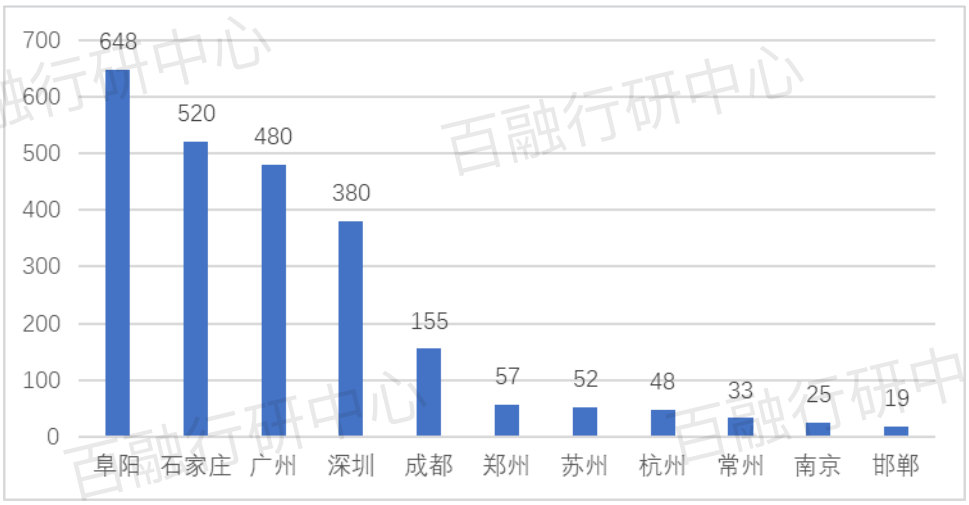
图52：中介群分布地统计



数据来源：百融行研中心

从QQ群统计到的成员主要分布地点观察，中介以及资信不良的高危人群主要集中在北京，共16,415人。占整个行业的9%。互联网金融平台的机构可以对北京进件的申请人进行重点关注，防止团伙欺诈。

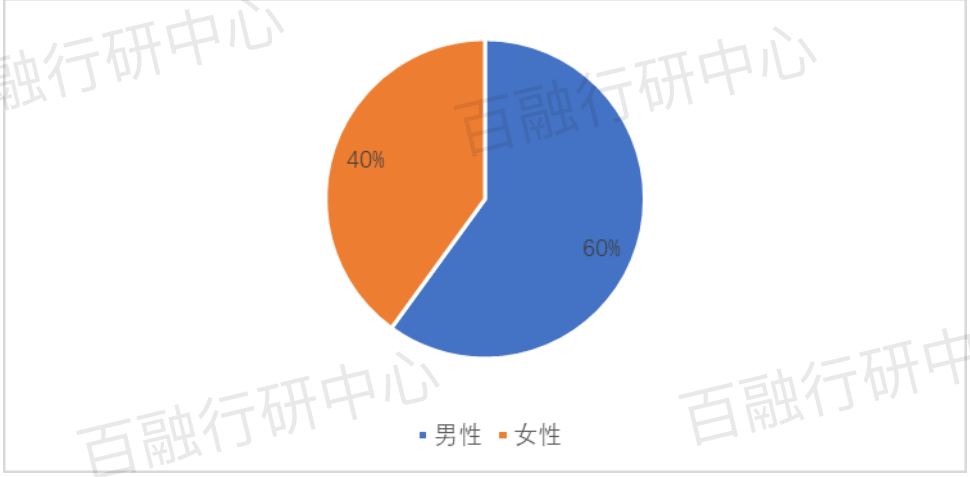
图53：中介群成员分布统计（北京除外）



数据来源：百融行研中心

除北京外，黑中介群成员要分布在阜阳、石家庄、广州、深圳、成都、郑州、苏州、杭州、常州、南京、邯郸等城市，金融机构可适当提升针对这几个城市的风险预警级别。同时要留意的是，广州、深圳、郑州、杭州既是中介群的发起地，也是中介群成员分布集中的地区，在制定反欺诈风险政策的时候需要更加严格谨慎。

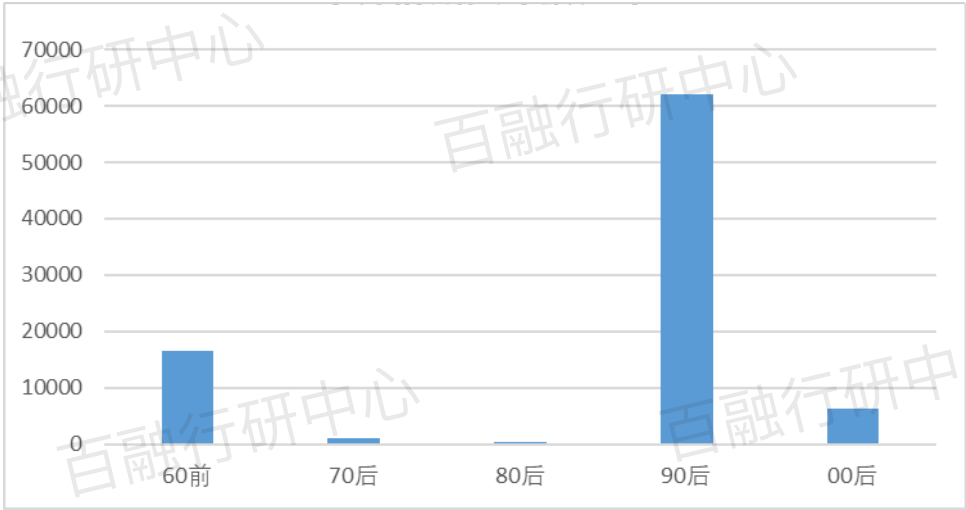
图 54：中介群性别比例



数据来源：百融行研中心

从性别比例上来看，黑中介群的成员的男女比例为 6：4，女性在中介从业者中占有相当大的比例。通过 QQ 搜索“口子”得出的 146 个 QQ 群当中，有 11 个群由女性中介从业者控制运营，可见女性在金融欺诈行业中扮演愈发重要的角色。

图 55：中介群成员年龄分布



数据来源：百融行研中心

在中介 QQ 群成员当中，公布年龄段的成员共 86,353 人，根据年龄分布统计，90 后的人数最多，占比达 72%，是中介的主要参与者。值得关注的是，60 后的中介群体占比达到 19%，排列第二，该群体年龄都在 58 岁以上，金融机构可适当提升对退休或即将退休客户群的风控标准。同样值得关注的是 00 后的中介人数占比 7%，排列第三，目前 00 后群体年龄均在 18 岁或以下，大多尚未成年。银行或者持牌消费金融机构可针对在学校开展的信用卡或者消费信贷业务寻求校方的协作，确认申请人为本校学生且无不良的历史记录。

04 盗刷盗号

四、盗刷盗号

盗刷盗号是指黑客利用金融平台的安全漏洞进而获得用户的金融账户、密码等信息，并提供给欺诈分子进行盗刷的行为。获取用户金融账户的方式主要有：（1）通过在 ATM 机上安装银行卡信息采集器或者通过非接触式银行卡采集器获取银行卡信息，并利用空白银行卡进行复制；（2）通过 POS 机的交易记录获得银行卡信息，并利用空白银行卡进行复制；（3）黑客通过技术手段获得银行卡密码以及其它金融账户信息。

跟身份盗用的信贷欺诈不同，盗刷盗号无需获得申请人身份证信息，且由于金融机构给与的金融账户在使用时仅需输入登录密码、交易密码即可，无需进行身份验证，获得用户金融账户以及密码，就相当于获得用户身份。所以盗刷盗号比冒用身份信贷欺诈成功概率更高。

盗刷盗号常用的技术手段为拖库、洗库和撞库，接下来我们将着重详细介绍每一个技术手段的流程和原理。

4.1 拖库

拖库也称“脱裤”，是欺诈分子通过技术手段或者社会工程的方式盗取用户信息的行为。拖库的步骤如下：第 1 步，黑客对目标网站进行扫描，查找其存在的漏洞，常见漏洞包括 SQL 注入、文件上传漏洞等；第 2 步，通过该漏洞在网站服务器上建立“后门 (webshell)”，通过该后门获取服务器操作系统的权限；第 3 步，利用系统权限直接下载备份数据库，或查找数据库链接，将其导出到本地。

拖库中有价值的信息包括：账号、密码、密钥、身份证号、电话通讯录以及任何与个人相关的信息。

4.1.1 技术攻击

拖库的技术手段包括利用 web 应用及服务器漏洞、远程下载数据库文件、水坑攻击④、XSS 劫持⑤。

针对通过技术手段进行拖库的行为，网站需要对数据库进行加密保护，并定期进行对网站篡改、网站挂马⑥等行为进行监控检查。

4.1.2 社会工程学

社会工程学，是一种通过人际交流的方式，对目标心理弱点、本能反应、好奇心、信任、贪婪等心理设置陷阱并骗取所需要的信息，并通过密码心理学、逻辑分析等方法刻画用户画像的行为，是非技术渗透手段。通过这种手段进行拖库非常有效，而且应用效率极高，社会工程学已是企业安全最大的威胁之一。

④ 水坑攻击：黑客分析攻击目标的上网活动规律，寻找攻击目标经常访问的网站的弱点，先将此网站“攻破”并植入攻击代码，一旦攻击目标访问该网站就会被盗取信息。

⑤ XSS 劫持：web 应用中的计算机安全漏洞，允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。

⑥网站挂马：黑客通过各种手段，包括 SQL 注入、网站敏感文件扫描、服务器漏洞、网站程序 0day 等各种方法获得网站管理员账号，然后登陆网站后台，通过数据库“备份 / 恢复”或者上传漏洞获得一个 webshell。

社会工程学的拖库攻击方式主要有邮件钓鱼（Spear-Phishing）攻击、网站钓鱼（Website Attack）攻击、群发邮件（Mass Mailer）攻击、伪造短信（SMS Spoofing）攻击以及近期发现的伪基站攻击。另外，社会工程学还包括熟人伪装、面试伪装以及通过身份伪装跟公司员工交谈的方式，套取公司系统信息。

预防社会工程学的攻击，需要加强对欺诈手段的认识与了解，提升对异常邮件、信息的警惕，并做好公司内部的相关安全教育。同时要完善规范公司的信息安全制度，防止敏感信息的泄露。

4.2 洗库

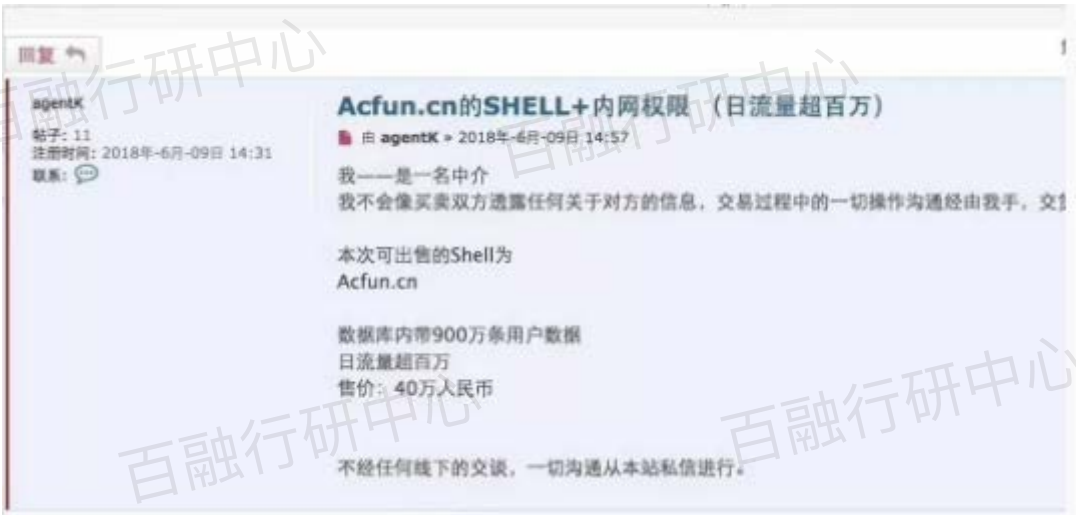
“洗库”，是指黑客、欺诈分子在完成拖库后，通过技术手段将有价值的用户数据归纳分析，变卖给黑产、欺诈分子变现的行为。

在黑客、欺诈分子完成“撞库”后，会将获得的信息分成四类：（1）金融类账户；（2）姓名、身份证、手机、邮箱、住址、QQ 等个人信息；（3）游戏账号；（4）其它信息。黑客会将信息在暗网中售卖给黑产或者欺诈分子。欺诈分子利用伪基站的方式获得申请人手机号、短信信息，再通过黑客或者黑产渠道获得对应的个人信息以及金融账户信息，然后通过网银或者其它线上金融渠道，将金融账户的资金转入自己的银行账号提现或者直接进行大额消费。

案例 1：

某动漫直播视频网站的用户数据在暗网出售，包含用户名、手机号以及密码，数量高达 900 万条，大部分为一手数据，出卖价格为 40 万人民币。如果这 900 万条信息，平均每条能获利 2 毛，欺诈团伙将有 140 万元的利润。

图 56：洗库案例（1）



数据来源：百融行研中心

案例 2：

浙江省 1,000 万学籍数据在暗网出售，包含了学生姓名、身份证、学籍号、户籍位置、监护人、监护人号码、居住地址、出生地、学校名称以及照片链接，数据在 100G 左右，利用比特币进行交易。如果这 1,000 万条数据当中，有 1,000 个学生上当，每个学生平均损失金额为 1,000 元，则欺诈份子收益达到 100 万元。

图 57：洗库案例（2）

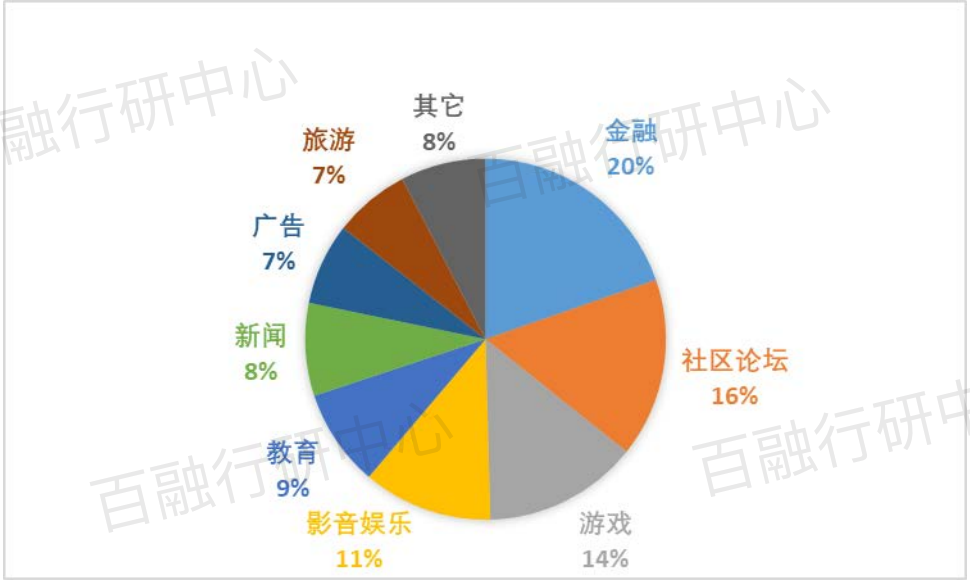
数据来源：百融行研中心

4.3 撞库

完成洗库后，黑客在售卖个人信息的同时，会将该部分信息进行整理，批量尝试在另一网站或平台匹配登录的行为，称为撞库。

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，尝试批量登陆其他网站后，得到一系列可以登录的用户。很多用户在不同网站使用的是相同的帐号密码，因此黑客可以通过获取用户在 A 网站的账户从而尝试登录 B 网址。黑客在进行拖库与洗库后，一般会利用已获得的用户信息进行撞库，已获取更多的用户信息。

图 58：被撞库网站行业分布



数据来源：阿里安全报告；数据整理：百融行研中心

根据阿里安全报告统计，截止至 2017 年，被撞库的网站当中，金融机构占比 20%，在所有行业中排行最高。根据对大量黑产撞库数据的统计，能够成功绕过风控策略的攻击占总攻击量的 83%，撞库成功率则在 0.4% 左右浮动。

部分金融机构网站在输入一次验证码后可进行多次登录尝试，黑产往往会利用所有和后端数据库存在交互的端口进行“check-user-exist”的尝试，故而建议网站验证码可做如下业务逻辑调整：

（1）判断账号是否存在

① 注册接口快速验证

许多网站在填写注册信息时，会通过 AJAX⑦对账户名是否可用做实时验证，如果可用便在页面上打勾，该接口大量被黑客用来判断某用户名是否有在网站注册。建议金融机构在网站登录时，避免使用 AJAX 进行账户验证，且每次登陆都需要重新请求验证码，避免出现一个验证码可进行多次登陆验证的操作。

② 登陆接口返回信息

部分网站如果账号密码错误会返回敏感信息暴露账号存在情况。例如返回提示「账号不存在」或「密码错

⑦ AJAX：指一种创建交互式网页应用的开发技术，可以在不重新加载整个网页的情况下，对网页的某部分进行更新。

误」，便能让黑客判断账号是否存在。此处我们推荐的返回信息显示为「账号或密码错误」。

③ 找回密码接口

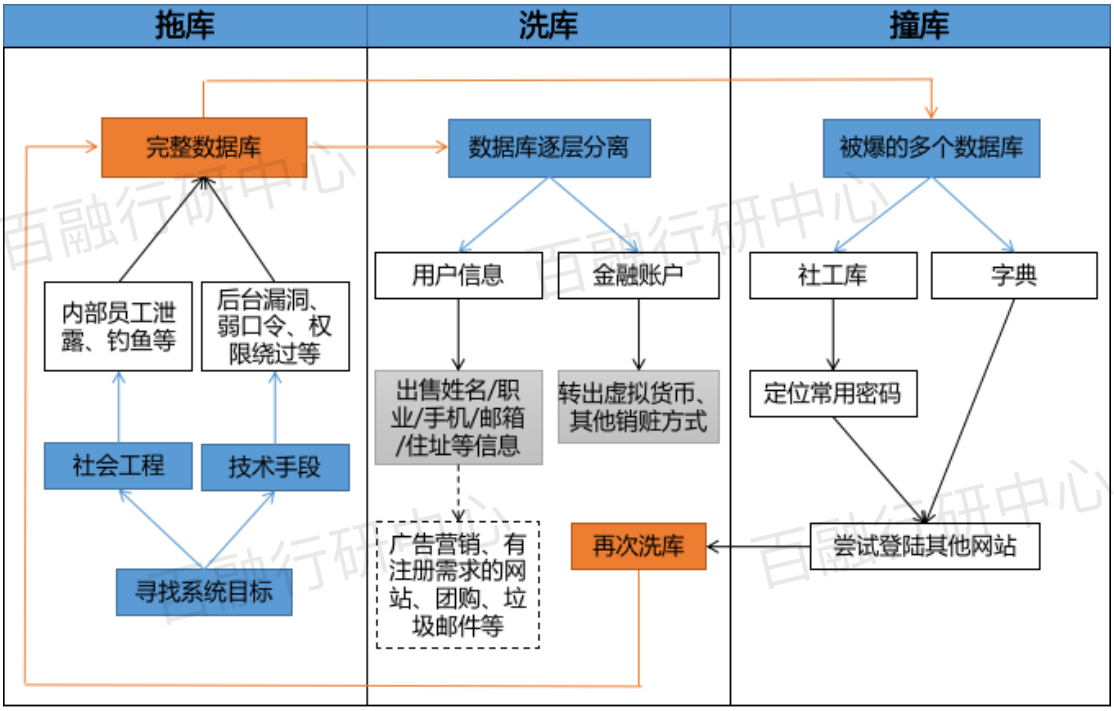
部分网站在找回密码的流程中，填写手机号或邮箱后会有一次带「账号不存在」提示信息，此处也常常被黑客用来判断账户存在与否，建议金融机构将返回信息删去。

（2）业务安全的集中管理

许多网站的主登陆口往往有比较严格的审计措施，会根据登陆 IP、频率等触发验证码或封 IP。但当公司业务增多，安全管理复杂度大幅增加，不同子站各用一套自己登陆验证，缺乏统一登陆接口的问题便会暴露。比如某个子产品的登陆功能，或者公司网站挂个论坛，往往会走单独的登陆接口，当这些边缘业务接口没有接入审计功能，便成为黑客攻击的温床。

从我们捕捉到的攻击数据中可以看到很多此类情况，黑客被对抗多次后都能再次发现新的毫无风控逻辑的撞库接口，甚至有的登陆接口公司安全部门都不知道其存在。所谓千里之堤，毁于蚁穴。尽管主业务做了大量的防御措施，当边缘业务出现疏忽时，一切措施便形同虚设。

图 59：拖库、洗库、撞库流程



数据来源：百融行研中心

以上，我们了解了三大欺诈种类的详细流程和相关信息，对于羊毛党来说，黑卡运营商、手机卡商、猫池厂商、收码平台、打码平台、改机工具以及群控工具等是其欺诈的主体和关键工具；而对于信贷欺诈，我们主要从欺诈类型、手段以及从业者画像进行了行业勾画；最后对于盗刷盗号，拖库、洗库和撞库是这个部分的主体模块。

针对于以上介绍的三大类欺诈类型，百融云创深耕信贷风控行业多年，愿意把我们的解决方案与行业经验进行分享，下一部分我们将展开介绍。

05

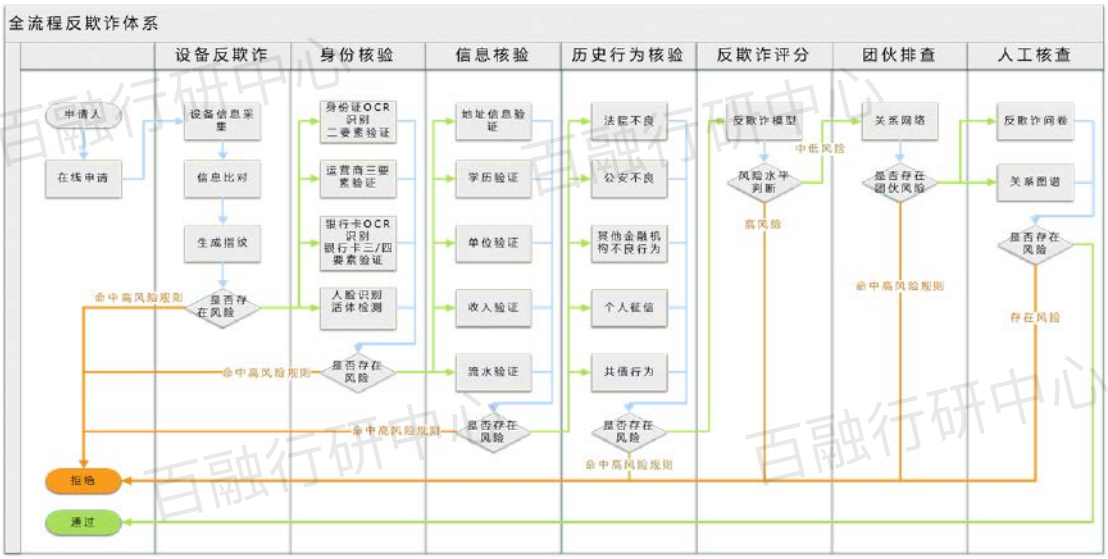
百融反欺诈解决方案

五、百融反欺诈解决方案

以上，我们按照市场黑产介绍了目前金融机构在面对市场外部环境风险时，主要会涉及哪些方面的欺诈攻击。在第五部分，我们将梳理整个贷前流程，在贷前申请人进件时，相关机构会面临的欺诈风险有哪些，以及针对这些风险，百融能从哪些方面协助机构进行有效防范。

如图 60，我们将贷前欺诈风险筛查分为 7 大板块：设备反欺诈、身份核验、信息核验、历史行为检验、反欺诈综合评分、团伙欺诈排查以及人工审批部分。设备反欺诈主要针对申请人申请设备是否存在异常来评判风险情况，而身份和信息核验主要针对申请人是否本人以及提供的基本信息是否可信等，在以上三个环节检验完成后，会从申请人的历史借贷行为查看客户是否出现过不良和高风险行为，这个阶段筛选后会从综合的欺诈评分以及关系网络查验申请人总体是否存在欺诈风险以及是否属于团伙欺诈类客群。在这些自动化决策筛选完毕后，最后进入人工。

图 60：全流程反欺诈体系



数据来源：百融行研中心

那么下面我们就以上流程涉及的欺诈风险，依次来看百融在整体流程中能起到哪些关键作用。

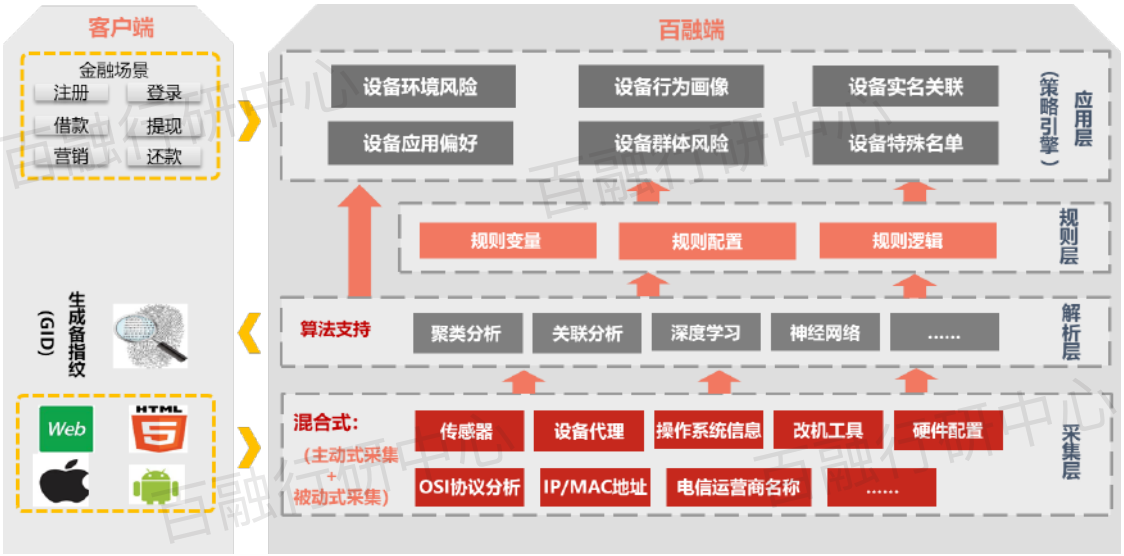
5.1 欺诈风险防控 – 设备反欺诈

欺诈分子会利用技术手段对机构网站以及申请入口等漏洞进行攻击，同时也会直接盗用客户账户，以妨碍

机构业务正常开展并使用户及机构方遭到损失并从中获利。

针对欺诈分子技术手段的攻击，百融推出谛听设备反欺诈。百融谛听设备反欺诈通过部署 JS 代码或者 SDK 代码在客户端主动地收集与设备相关的信息和特征，如采集浏览器、设备配置等，同时传令被动式共同采集设备信息，并利用聚类分类、关联分析等算法生成百融设备指纹（GID），通过识别设备端的环境风险、行为画像、实名关联、应用偏好、群体风险等来预防群控、撞库、盗号等欺诈风险。在传统的设备指纹基础上，谛听设备反欺诈新增传感器、改机工具运行状态、页面停留时长，开机时间等的采集判断，提升设备识别的准确度以及召回率，可应用在注册、登录、借款等多个环节。

图 61：百融谛听设备反欺诈架构



数据来源：百融行研中心

百融谛听设备反欺诈特点：

◆ 唯一性稳定性更强，不易篡改：主动式采集与被动式抓取相结合。

◆ 同一设备跨平台打通：百融根据多年设备指纹经验，凭借着过硬的技术能力，通过客户端采集设备非敏感信息特征，联合服务端 OSI 协议栈分析，打通同一设备中 app 与 web 之间的平台壁垒，实现一台设备终身唯一 GID，且稳定性更强，不易篡改。

◆ 群控设备实时识别：通过分析群控设备的多种环境特征，操作习惯，采用前端采集传感器信息加后端算法实时分析，能够准确实时识别设备是否属于群控设备。

谛听反欺诈设备指纹 GID 总体支持情况展示：

◆ 设备指纹稳定性和唯一性

图 62：GID 的唯一性和稳定性

功能	场景	效果
唯一性	1. 不同设备生成不同的设备指纹	Pass
	2. 同一设备不同 APP 生成相同的设备指纹	Pass
稳定性	1. 切换网络类型	Pass
	2. 杀掉应用进程重新打开	Pass
	3. 禁用软件相关权限	Pass
	4. 手机重启	Pass
	5. 应用卸载重装	Pass
	6. 更新应用	Pass
	7. 恢复默认出厂设置	Pass
	8. 一键刷机	Pass
	9. 改机工具（修改设备基本信息）	Pass

数据来源：百融行研中心

首先 GID 会对应不同设备生成不同设备指纹，但只要百融底层算法定位为同一设备的情况下，即使设备使用人通过不同应用生成 GID，对应生成的设备指纹都是跟着设备走的，同一设备只会有一个 GID。同时，从稳定性来看，不论是不同网络切换、手机重启、应用更换、恢复出厂等任何操作，GID 具有稳定性。

- 设备指纹唯一性及稳定性测试详情

下面，我们仍然以 Android 系统为例，来看下百融 GID 的稳定性表现（改机工具部分百融谛听设备反欺诈 GID 稳定性测试请参考第二部分中改机工具欺诈风险部分的对应解决方案内容）。首先我们在标准环境下生成百融 GID（“443330001001536651735363450334 5”），如下图：

图 63：原始 GID

数据来源：百融行研中心

当我们切换网络类型并查看 GID 是否有变化时，结果是不论是在 4G 网络还是 WIFI 情况下，GID 都是“443330001001536651753634503345”

图 64：切换网络环境后的 GID

WIFI 环境下　　4G 环境下

数据来源：百融行研中心

当我们彻底结束谛听设备反欺诈应用进程后看 GID 是否有变化，结果 GID 仍然保持为“4433300010015366517353634503345”：

图 65：彻底结束设备反欺诈进程后的 GID

数据来源：百融行研中心

接着，我们看下在禁用百融谛听设备反欺诈应用后 GID 是否有变化，结果 GID 仍然保持为“443330001001536651753634503345”：

图 66：禁用谛听反欺诈后的 GID

数据来源：百融行研中心

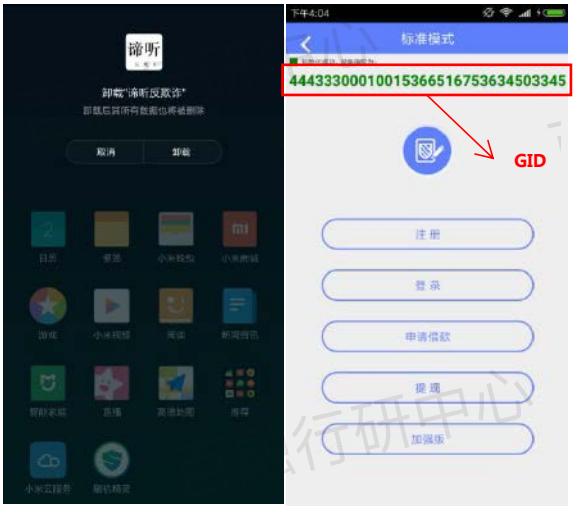
手机重启对 GID 的影响，我们发现在设备重启后 GID 仍然保持为“443330001001536651735363450334 5”：

图 67：卸载设备反欺诈后的 GID

数据来源：百融行研中心

我们尝试卸载百融谛听设备反欺诈程序后 GID 是否变化，结果卸载后 GID 仍然保持为“443330001001536651735363450334 5”：

图 68：设备重启后的 GID



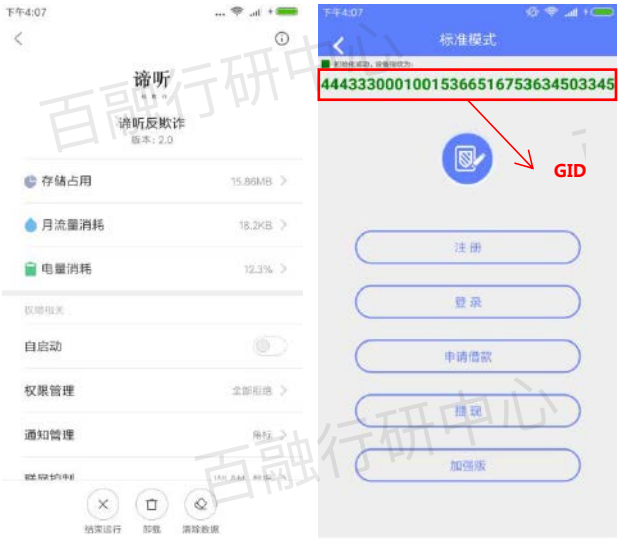
数据来源：百融行研中心

同时，我们还可以看看，在百融谛听设备反欺诈产品更新后，对于 GID 是否产生影响，如图 69（版本 1.0）和图 70（版本 2.0），结果 GID 仍然保持为“443330001001536651735363450334 5”：

图 69：恢复出厂设置后的 GID

数据来源：百融行研中心

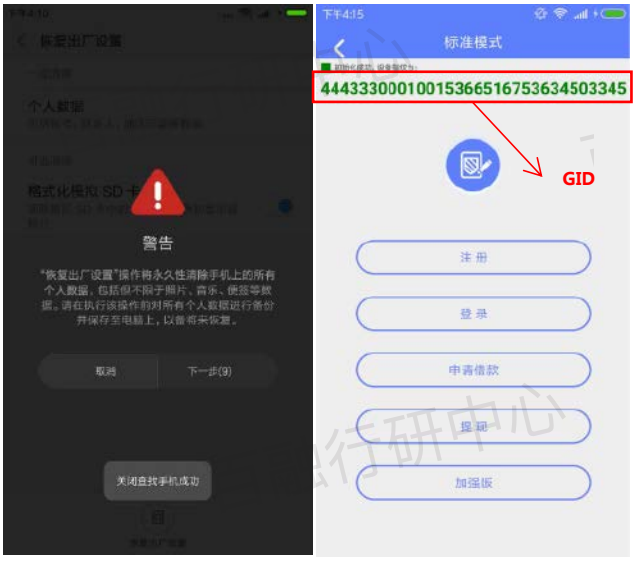
图 70：刷机后的 GID



数据来源：百融行研中心

即使是恢复出厂设置，GID 仍然保持为“443330001001536651735363450334 5”：

图 71：设备反欺诈 1.0 时的 GID



数据来源：百融行研中心

同时，如果直接进行刷机处理，如图 72 左图启动刷机功能后，图 72 右图中的 GID 仍然保持为“443330 0010015366517353634503345”不变：

图 72：设备反欺诈 2.0 时的 GID

数据来源：百融行研中心

- 设备环境风险识别

图 73：百融谛听设备反欺诈环境风险识别

功能	场景	效果
模拟器识别	使用夜神，雷电等模拟器运行	Pass
VPN 代理识别	使用 VPN 代理访问	Pass
HTTP 代理识别	使用 HTTP 代理访问	Pass
是否 root 识别	使用 root 过的手机访问	Pass
改机工具安装识别	使用安装改机工具的手机访问	Pass
改机工具使用识别	使用使用改机工具的手机访问	Pass
模拟位置识别	使用模拟地理位置的手机访问	Pass
群控设备实时识别	使用群控软件控制手机访问	Pass

数据来源：百融行研中心

从百融谛听反欺诈能识别的环境风险来看，模拟器、改机工具及群控设备均能进行识别。

- **设备环境风险识别测试**

下面我们仍然以 Android 系统为例，来看下对于设备环境风险，百融设备反欺诈是怎么来进行评判的。

首先，以雷电模拟器为例，从图 74 中可以看出，在运行雷电模拟器以后，该设备中我们探测出了模拟器的运行（“是否为模拟器”结果为“是”）：

图 74：模拟器识别

数据来源：百融行研中心

同时对于 VPN（图 75 图 2 显示为“是 vpn 登陆”）和 HTTP（图 75 图 4 显示为“是 HTTP 登陆“）这种代理登陆来说，可以看出，百融也是可以轻松进行标记识别的：

图 75：VPN 和 HTTP 代理识别

数据来源：百融行研中心

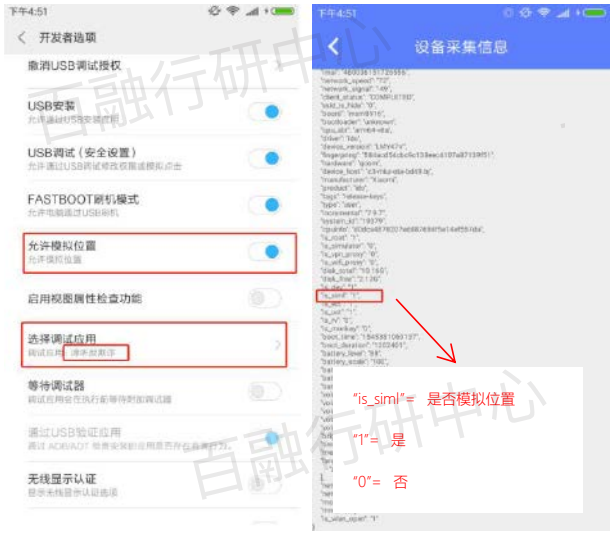
而当设备越狱且进行登陆时，百融也可以进行准确识别，如图 76 左图中，使用刷机精灵后，右图“是否越狱”结果为“是”：

图 76：ROOT 识别

数据来源：百融行研中心

而假设申请人使用设备开启模拟位置功能时，即避免被申请机构探测到真实或即时地址时，百融也是可以迅速做出判断的，如图 77，该设备开启模拟位置功能时，右图设备采集信息中“是否模拟位置”显示为“是”：

图 77：模拟位置功能识别



数据来源：百融行研中心

最后，关于设备环境风险的还有群控设备的识别，下面我们现在相关设备上安装群控软件 TOTALCONTROL，然后探测该设备的风险状况：

图 78：TOTALCONTROL

数据来源：百融行研中心

如图 79 显示，我们发现该设备有群控设备风险，因为“是否群控设备”显示为“是”：

图 79：群控设备识别

数据来源：百融行研中心

- 安全性

图 80：GID 的安全性

功能	场景	效果
安全性	是否控制代码混淆	Pass
	是否反编译后代码可读	Pass
	传输数据中是否防篡改	Pass
	传输数据中是否加密	Pass

数据来源：百融行研中心

GID 在传输过程中安全性也是有一定保证的，首先会严格控制代码混淆的情况出现，其次在传输过程中会进行加密且带防篡改功能。

5.2 欺诈风险防控 - 身份核验

虚假身份是指通过购买真实自然人信息进行骗贷的欺诈行为，即冒用。因为信息真实，普通反欺诈手段无法识别。普通的人脸识别技术黑产也有了“过脸产业”与之相抗衡，即帮无法完成账号实名认证的人群完成实名认证并获取利益。

图 81：百融身份验证解决方案

数据来源：百融行研中心

为防止贷款借款人冒用他人信息，提供虚假身份，需要对贷款借款人的身份进行核实，身份验证作为反欺诈的第一道防线，是对信贷借款人的信息做确认。由于银行卡四要素是申请人在银行开户面签时留下的资料，通过银行卡四要素验证 + 人脸识别进行验证，能够较为有效的防止身份盗用；针对信用卡发卡等无需绑定还款卡的网申场景，可以通过运营商三要素验证 + 人脸识别进行初步验证，然后结合其它反欺诈手段进行综合判断，如通过手机在网时长 / 在网状态以及设备信息来识别借身份冒用的风险。

5.3 欺诈风险防控 - 信息核验

虚假信息是指真实的借款人通过包装身个人工作、家庭、联系人、财力信息等进行骗贷的欺诈行为。部分申请资料虚假欺诈是个人行为，但绝大多数资料包装是有中介或者欺诈团伙参与的。

对于中介资料包装，机构可通过让申请人提供工作、收入以及财力证明并进行人工核实，也可以通过百融来检验申请信息的真实性。除了能够对申请人填写资料的真实性进核验，还能通过申请人工作稳定时长、工作跟家庭地址的变动频率以及是否为高风险地址等维度对申请人的欺诈风险进行综合评估。机构可以通过申请人资料、单位资料以及地址资料的三方检验进行对比，能够有效的防止资料包装、造假的行为，提升自动审批率以及通过率，并降低欺诈风险。

5.4 欺诈风险防控 – 历史行为核验

针对于有不良历史记录的申请人，可通过百融公检法信息核查、特殊名单、信贷意向、实名信息核查以及反欺诈评分进行综合判断。

特殊名单验证

包含本人、社会关系人在银行、小贷、P2P 和消费金融机构是否存在历史不良纪录、命中次数及最近一次命中时间，包括短时逾期、不良、资信不佳、拒绝和失联等。其中高危行为、法院失信人、银行 / 非银机构中高风险为较为严重的风险类型，机构可以做直接拒绝，其它类型的特殊名单，机构可以结合其它策略进行评估。

图 82：百融特殊名单分类

匹配方式	无机构划分		银行/非银（P2P、小贷、消费金融等）				
	高危行为	法院失信人	中风险	一般风险	资信不佳	高风险	拒绝
按本人**身份证**查询	疑似团伙欺诈，**建议拒绝**	**建议拒绝**	曾有坏账，**建议拒绝**	曾有短时逾期，建议**关注或综合考虑**	有资料不实历史，建议**关注或综合考虑**	曾有失联，**建议拒绝**	其他机构拒绝，建议**关注或综合考虑**
按本人**手机号**查询							

数据来源：百融行研中心

法院不良信息

覆盖最高法以及省市各级法院的最新公布名单，包括执行法院、立案时间、执行案号、执行标的、案件状态、执行依据、执行机构、生效法律文书确定的义务、被执行人的履行情况、失信被执行人的行为等信息。行

方对于命中法院不良信息的申请人需要结合案件性质以及时间综合判断，考虑是否拒绝申请。

借贷意向验证

基于个人在金融机构中出现的多次申请的情况进行分析，评估个人的共债倾向。包括近 7 天、近 15 天、近 1 个月、近 3 个月、近 6 个月、近 12 个月，同时支持当日申请核查。银行客群质量较好，平均申请次数较低，若申请人近一个月在非银行机构内有 3 次或以上申请记录，出现坏账的概率会明显高于一般客户。

实名信息验证

查看申请人关联信息是否涉及团伙性欺诈或疑似黑中介等行为，如一个手机号在一个月内关联 3 个或以上身份证号，则有可能是中介作案或者团伙作案。

5.5 欺诈风险防控 – 反欺诈评分

百融基于逻辑回归算法，开发了相应的客群评分模型，适合冷启动客户快速开展业务。

当金融机构积累了一定的欺诈样本及表现期后，可开发专属于金融机构的定制化模型。

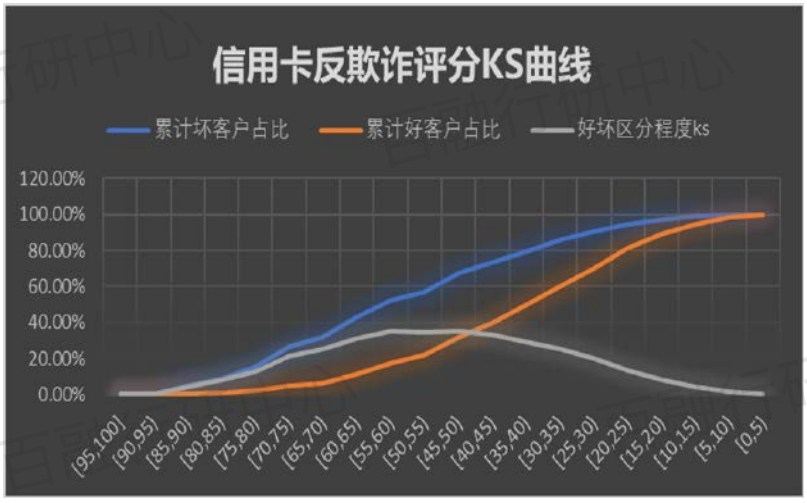
风险策略：分值在 0~100 分之间，分数越高欺诈风险越高，违约的可能性越高，不同的客群审批策略有所不同。

以下是百融反欺诈规则、评分在银行测试的实际情况。行方先拒绝命中百融反欺诈高风险规则的客户，然后用反欺诈评分再次进行筛选，ks 值依然能达到 0.44：

图 83：反欺诈评分分布示例

数据来源：百融行研中心

图 84：反欺诈评分 KS 值



数据来源：百融行研中心

5.6 欺诈风险防控 – 团伙欺诈

（1）团伙欺诈定义

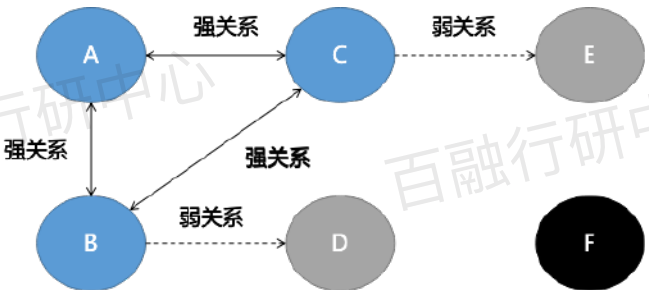
团伙欺诈是指利欺诈分子有组织、有目的、有计划的对金融机构进行批量的欺诈申请。由于欺诈成本较高，故团伙欺诈一般会有多套共用信息 ,通过信息的错配 ,利用机构间信息孤岛的缺陷进行大规模、多平台的集中攻击。

（2）关系图谱逻辑

世界上的事物都是由各类实体所构成的，比如，世界上的每个人是一个实体，世界上的所有人则构成了人这个实体类；又比如，世界上的每家金融机构又是一个实体，世界上的所有金融机构则构成了金融机构这个实体类。

实体与实体之间并不是孤立的，他们由各种各样的关系关联起来，正所谓“万物互联”。这种关系可以是同一实体类内的实体关系，也可以是不同实体类内的实体关系，如图 85，在人这个实体类内，人与人之间的关系可能是强关系（如同事关系、朋友关系、师生关系等）、也有可能是弱关系（如三度以上关联人）、还有可能没有任何关联。

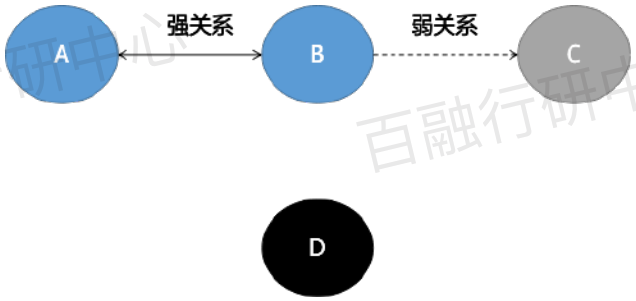
图 85：个人关系网络样例



数据来源：百融行研中心

又如图 86 ,在机构实体类内有强关系(例如母子公司关系 ,有兄弟公司关系、有合作关系等)、也有弱关系(例如三度关系以上等) 或者没有关系：

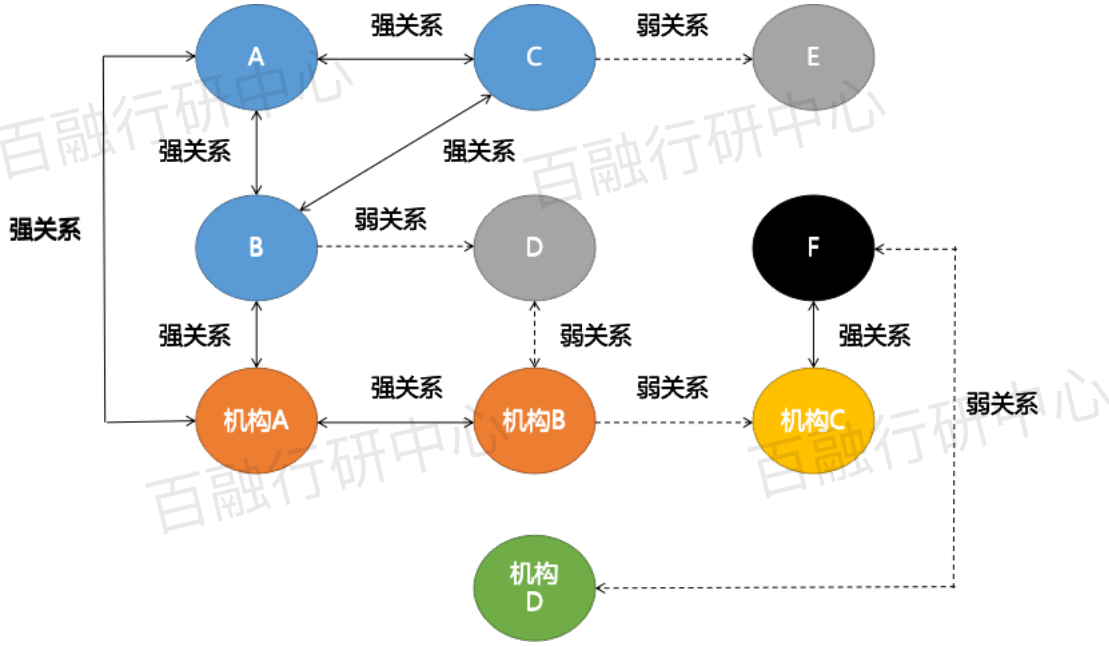
图 86：机构关系网络样例



数据来源：百融行研中心

事实上，我们可以把表示不同实体与关系的多个图叠加形成一个大图，并且可以在该大图上定义不同类的实体之间的新的关系，我们把这样混合多个实体与关系的图称之为图谱，如图 87，这样我们就得到了一个简单的关系图谱，他包含两类实体：个人和机构，三类关系：强、弱和无关系：

图 87：关系图谱样例



数据来源：百融行研中心

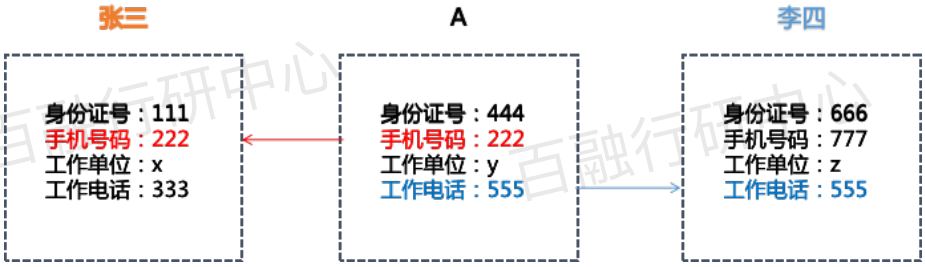
我们把图谱包含实体类和关系类的集合称为关系图谱的本体 (Ontology)，其给定了关系图谱的结构，是关系图谱对现实世界的抽象反映。总而言之，关系图谱就是一个多实体、多关系图。

（3）关系图谱在团伙欺诈中的运用

■ 一致性检验

一致性检验的思路就是尝试推导出申请人信息与关系图谱不一致的地方，不一致的、矛盾的地方越多，申请人欺诈的嫌疑越大。对于团伙欺诈，有些时候各个申请人之间会存在不合理或自相矛盾的地方，如果我们能够有效地找出不合理或不一致的线索，将有助于识别欺诈行为。

图 88：申请人 A 信息验证



数据来源：百融行研中心

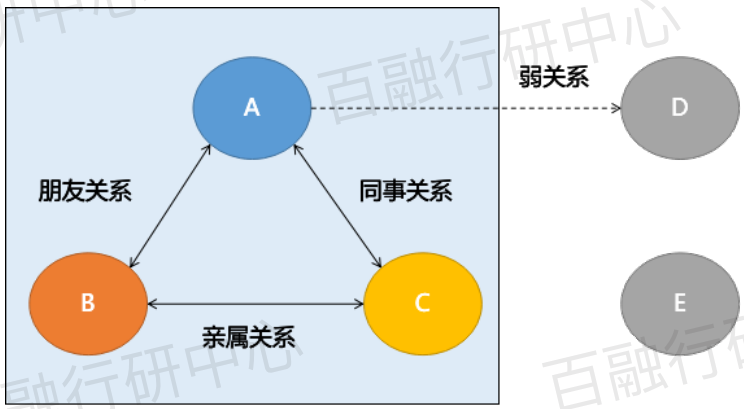
假设我们拥有且确认张三和李四的已知基础信息（如图 88 所示），此时有新申请人 A，从图中匹配结果可以发现，申请人 A 和张三存在身份证不相同但手机号却相同的情况，一般情况下，手机号都是实名制的，所以这里存在信息不一致的情况；同时，申请人 A 与李四的公司名称不同但公司电话却相同，所以这里也存在信息不一致的情况。综合来看，申请人 A 的欺诈风险很高，可能是团伙欺诈也有可能是代办包装。

■ 团伙欺诈检测

除了一致性验证，对团伙欺诈来说，我们还可以利用更有针对性的团伙识别算法，通过团伙识别算法可以有效识别出申请人是否属于某一团伙，如果更进一步，我们还能确认该团伙是否属于欺诈团伙，如果是这样那么该申请人是欺诈的嫌疑就很大了。

首先，我们需要在个人实体集上识别出团伙。团伙可以看成是具有相对紧密关系的个人实体的集合，比如，图 89 关系图谱中，A、B、C 互为亲密关系，他们之间关系明显比 D 与 E 要来的紧密，因此，我们可以判定他们属于一个团伙。在实际应用中，我们可以综合图论算法、关联挖掘算法、机器学习算法来建立我们的团伙识别算法。

图 89：关系图谱样例



数据来源：百融行研中心

其次，当我们识别出团伙后，还需要判断该团伙是否欺诈团伙，有一种方法是建立一个团伙风险相关的指标，若团伙的指标大于阈值，例如团伙关联欺诈信息或者异常信息越多，综合评分越高，当高于一定风险水平时，即判定为团伙欺诈。另一种更简单有效的方法是动态维护一个欺诈种子库（欺诈名单），若团伙包含有欺诈种子，即可判断该团伙为欺诈团伙。在实际应用中，可以把两种方法结合达到较好效果。

■ 综合团伙欺诈风险评定

而当申请人可能不属于任何欺诈团伙，或者团伙欺诈在既定维度评定申请人风险较弱时，我们可以计算该申请人到最近的欺诈团伙的路径与距离等方法，比如，申请人亲密关系网络的关联信息个数或某类亲密关系的占比等，应用这些变量于建立申请客户欺诈评分与信用评分，去综合评判客户的团伙欺诈风险。

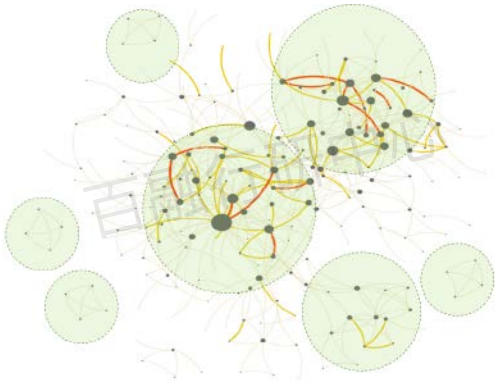
（4）百融关系图谱

依据上面的原理，同时依托知识图谱等算法技术将不同种类的信息连接在一起，从而形成百融关系图谱产品。

首先，百融对当前的欺诈手段与形势进行了充分的调研，结合了百融的海量数据，设计百融关系图谱的本体，即图谱所涉及的实体（如个人、贷款机构、电话号码等）与关系（如人与人的亲属关系，人与电话号码的所有关系等）。然后会根据所确定的关系图谱本体，在百融数据库抽取、清洗数据，并把数据转换成适当的形式，以图结构的组织方式进行存储，同时利用合理的算法计算关系图谱本体所定义的关系。对于识别出的团伙，百融还建立模型计算出其风险级别，风险级别越高表示团伙成员的关系越紧密，若该团伙是欺诈团伙，则表明该欺诈团伙的风险越高。关系图谱产品经过多轮测试与优化，能够较有效识别出高风险欺诈实体。

我们知道，不同的团体，显示的关系也有所不同。正常个体是独立的节点，或与另一个节点的组合（社交关系），所以正常关系的团体，通常呈现分散的状态。而欺诈团伙因有共享信息，所以会有聚类现象出现，如图 90 中骗贷团体和逾期团体的关系图谱就出现了聚类特征：

图 90：异常团伙欺诈关系图谱



数据来源：百融行研中心

（5）百融团伙欺诈排查案例

百融合作的一个银行客户提供了 5,000 个欺诈样本及 8 万个申请样本，通过百融撞库发现其中 9,000 多个客户疑似团伙型欺诈。运用百融关系图谱，关联出 18 万个团伙风险客户，其中有 7.96 万多客户在行方申请过贷款，其中 90% 申请客户在行方贷前反欺诈已拒绝，而剩余成功申请的 970 个客户的风险是平均坏账的 5 倍。如果能在贷前运用百融关系反欺诈进行有效识别，将大大降低银行风险，减少坏账。

图 91：团伙欺诈排查实际应用效果

数据来源：百融行研中心

（6）百融反欺诈关系图谱的特点与优势

首先，构建图谱的数据数量要足够多与全面，才能够使图谱逼近真实世界的全貌，否则只能是瞎子摸象得出错误的结论，在这方面，百融的数据库覆盖了中国七亿以上的人口，能够满足反欺诈的需求。

其次，运行与维护关系图谱的软硬件要求极高，如上所述，关系图谱的构建用到了海量数据，关系图谱的后续更新，查询同样需要处理海量数据，特别是查询操作要求快速响应，这对运行关系图谱的软硬件提出了极大挑战。目前百融公司的关系图谱产品运行稳定，图谱数据每天更新，查询响应速度能够满足互联网反欺诈需求。

最后，有效的关系图谱的开发需要规范的流程与成熟的方法论。在整个开发过程中，百融组织全公司相关技术骨干专家与工程师充分讨论与技术攻关，先制定周密、科学的开发方案与技术路线，然后严格按照规范，在强有力的后勤保障下组织关系图谱的开发与部署，最终取得了满意的成果。

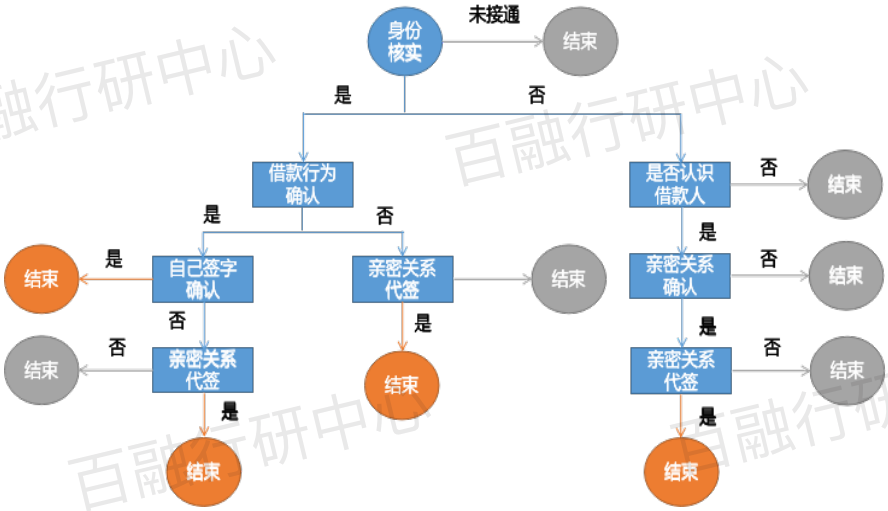
5.7 人工核查

在贷前防控流程的最后一步中，针对人工审批，百融可提供智能语音机器人以替代部分人工的工作，如审批和回访。而具体操作流程和逻辑，举个例子，在回访模拟中，智能语音机器人可通过图 98 中的流程案例对

借款人进行核实。

在类似决策树的机器人审批流程中，灰色部分为非正常借款核实情况，例如客户未接电话、否认自己有借款签字行为等，而橙色部分为正常借款情况，例如本人已签字或者亲属代签等。同时这些结果标签都会直接进入数据库，进行二次流转和处理。以此来节省人力成本且随性化审批策略。

图表 92： 机器人回访审核流程样例



数据来源：百融行研中心

06 总结

六、总结

在近几年内，金融科技在互联网和金融行业的环境下不断发展，越来越多的新技术种类和手段层出不穷，为整个金融行业提供了强有力的信息和风控能力补足。借助这些数据和服务，各类信贷机构可以从贷前更好地做出客户欺诈风险控制，百融云创深耕信贷风控领域多年，尤其在服务银行客户、消费金融、头部汽车金融公司等持牌机构上有业内领先优势。借助人工智能、大数据、区块链技术应运而生的大数据风控日臻成熟。在征信体系还不健全的当下，百融可以利用自身整体贷前反欺诈产品体系帮助相关机构将大数据风控与传统风控相结合，搭建属于机构自己的智能反欺诈风控体系，实现对申请人的高效全面欺诈风险防范。一个成熟的贷前风控体系大致分为前端欺诈风险识别以及信用风险识别两个板块。如果我们将具体的欺诈风险进行归类的话，可分为四大类：虚假身份、虚假信息、历史欺诈以及团伙欺诈，所以，在通过前端欺诈风险初筛时，针对这四大风险板块，百融可从五个维度进行全方位判别：谛听设备反欺诈（分别从设备环境、应用偏好、行为画像、群体风险以及设备黑名单等方面进行单规则或群体规则的欺诈风险评判）、身份信息验证（主要从身份信息的一致性进行把关）、实名反欺诈（主要从实名信息对应的黑名单、中高风险历史行为记录等进行评估）、百融反欺诈评分（主要从综合的维度评判申请人未来欺诈的可能性）以及评判团伙欺诈的核心产品关系图谱。最后再进行综合信用风险判别。

图 93：百融信贷业务贷前风控体系

数据来源：百融行研中心

反欺诈是一项长期的工作，反欺诈的技术手段在提升，欺诈分子也在不断优化攻击方式，金融信贷机构需要对黑产产业进行监控，才能做到知己知彼，百战不殆。 同时需要认识到欺诈行为是无法完全避免的，金融信贷机构需要做的是提高欺诈分子的作案成本，只有当整个行业的欺诈成本提高，欺诈分子认为无利可图，才会退出行业。最重要的一点金融信贷机构需要做好内控以及信息管理工作，很多欺诈风险都是由于信息安全以及人为的操作原因引起的，没有完善的内控以及信息安全体系，风控技术再完善也只会是亡羊补牢。

07 联系信息

七、联系信息

薛 婧
解决方案部 高级总监

电话： 185-1393-0409
邮箱：jing.xue@100credit.com

申宇峰
金融科技部 高级经理

电话 ：152-0136-1359
邮箱 ：yufeng.shen@100credit.com

孙梦芸
解决方案部 高级经理

电话 ：177-8064-5560
邮箱 ：mengyun.sun@100credit.com

许 可
解决方案部 高级经理

电话 ：180-2628-2069
邮箱 ：ke.xu@100credit.com

鸣谢：

此研报从选题到完成，得益于很多人的帮助与支持，首先在此衷心感谢季元总的大力支持以及黄嘉纶博士的专业咨询。除此之外，还要感谢冯鑫、吴国杰、张正媛、左红亮、靳璐杰、杨帆、马丁、叶子凡、胡莎、姜宁、叶娟以及林钦洁等人员对本研报的辛苦付出。

百融云创科技股份有限公司
地址：北京市海淀区科学院南路 2 号融科资讯中心
C 座北楼 20 层
电话：010-62508053
网址：http://www.100credit.com