经济下滑或露端倪 诈骗井喷蓄势待发

最难缠的羊毛党与其它诈骗

—— 揭开反欺诈3.0时代的序幕

演讲者：马骏驱
同盾科技联合创始人兼*CSO*

马骏驱（Jackal Ma)

- 出生于香港，香港大学电机与电子工程学士，05年获长江商学院第三届EMBA工商管理硕士学位。20多年工作经历遍布北美、大洋、亚洲、欧洲
- 历任IBM高级工程师
- 加拿大皇家银行技术规划部主管
- 香港八达通系统总架构师等职务
- 法国AXA保险集团亚太区区域运营主管
- EDIFY亚州JV总裁 / Aspect北亚区董事总经理
- 在国内先后参与众多大型企业如浦发 / 深发 / 建行 / 平安等大型企业的咨询与变革项目，同时被委任为多个国家单位（如工信部 / 发改委）的顾问。
- 2012年加入ThreatMetrix任亚太区副总裁
- 2014年加入同盾成为联合创始人，现任同盾 首席运营官
- **回国后致力打造一家立足中国，影响全球的反欺诈和风险控制大数据企业。**

警号

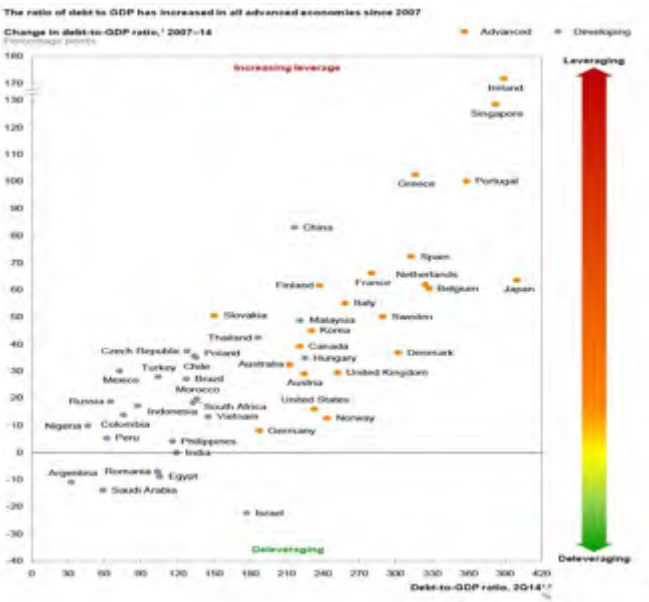
中国债务危机

2007年来翻了4倍

约50%跟房地产有关

影子银行年增长率36%

警号


The ratio of debt to GDP has increased in all advanced economies since 2007
Change in debt-to-GDP ratio,[1] 2007–14
Percentage points
Advanced
Developing
Increasing leverage
Deleveraging
Leveraging
Deleveraging
Debt-to-GDP ratio, 2Q14[1]
Ireland
Singapore
Greece
Portugal
China
Spain
Netherlands
France
Belgium
Japan
Finland
Italy
Slovakia
Malaysia
Sweden
Korea
Thailand
Canada
Czech Republic
Poland
Hungary
Denmark
Turkey
Chile
Australia
United Kingdom
Mexico
Brazil
Austria
Morocco
Russia
South Africa
United States
Indonesia
Vietnam
Norway
Nigeria
Colombia
Germany
Peru
Philippines
India
Argentina
Romania
Egypt
Saudi Arabia
Israel


BANK
BANK

警号

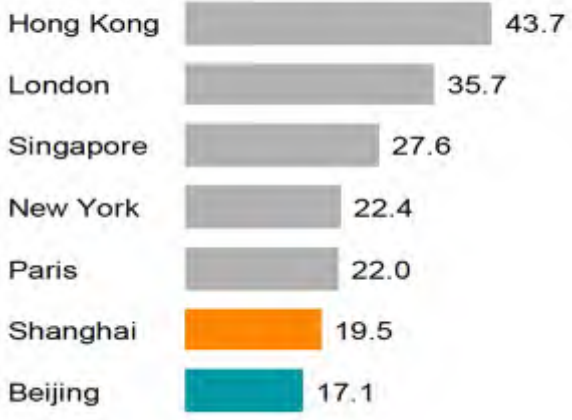
Exhibit 36

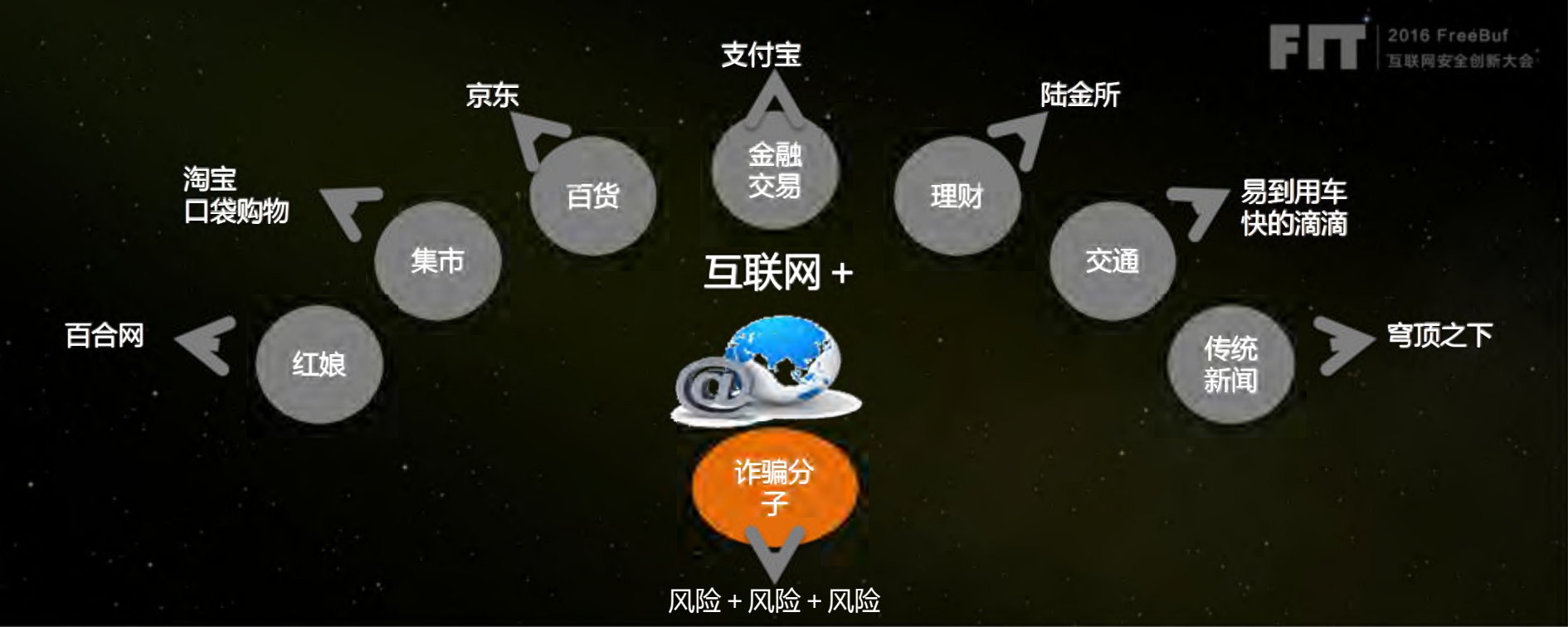
Nearly half of China's debt is related to real estate

Debt exposure to property, real economy 2Q14[1]
$ trillion

	Household[2]	Real estate sector	Real estate-related sectors[3]	Government[4]	Total exposure to property
As % of debt	8	10–15	10–15	10	40–45

Luxury residential property price in prime locations, 2013
$ thousand per square meter




支付宝
京东
陆金所
淘宝
口袋购物
金融
交易
百货
理财
集市
互联网 +
交通
易到用车
快的滴滴
百合网
红娘
传统
新闻
穹顶之下
诈骗分
子
风险 + 风险 + 风险

欺诈场景分析

欺诈场景(电商、信贷、理财)

账户盗用

账号+密码

单一的认证体系无法让企业百分百确信用户身份

欺诈场景(电商、信贷、理财）

账户盗用

可信设备ID访问
常用IP地址访问
机器行为识别
来源IP/真实IP对比、VPN检测
设备、IP、账户、地理位置多维度关联
强大的黑名单、灰名单库
.....

账号+密码

基于用户行为和设备智能的身份认证模型为企业把好账户登录关

欺诈场景（电商、支付）

盗卡支付
Stolen card

1 黑客通过钓鱼网站、木马病毒、漏洞攻击、社会工程、不法商户侧录等手段拿到银行卡、信用卡信息。

2 卡信息被卖至地下黑市或直接被用来进行欺诈。

3 欺诈分子从地下黑市买到被盗银行卡、信用卡卡信息。

4 欺诈分子在商户购买商品或服务。

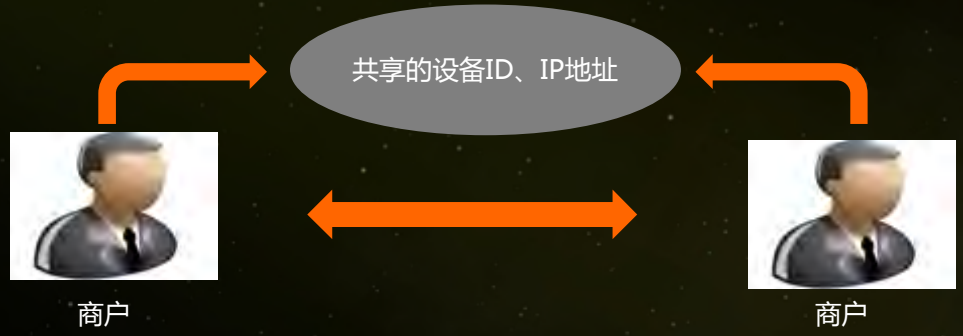
外卡支付中，只需输入卡号、有效期、CVV码，经常发生CNP欺诈。

5 几周后，卡的主人发现欺诈交易，打电话至银行处告知盗刷，要求召回。

6 商家和支付平台面临拒付损失（chargeback），品牌形象遭受破坏，严重时甚至需关闭业务。

欺诈场景（电商）

商户欺诈：自买自销，刷单提高信誉



欺诈场景（电商）

商户欺诈：与买家共谋，刷单提高信誉

谁	什么时间	什么环境	什么方式	谁	什么事情
 买家	交易 时间	设备ID IP 操作系统 浏览器属性	高频 小额 大量 代理IP	 商户	下单 创建交易 确认收货

欺诈场景（电商）

商户欺诈：与买家共谋，利用电商平台套现

买家账户1

买家账户2

相同的设备ID

大额、大量、非正常
商品、收货地址异常

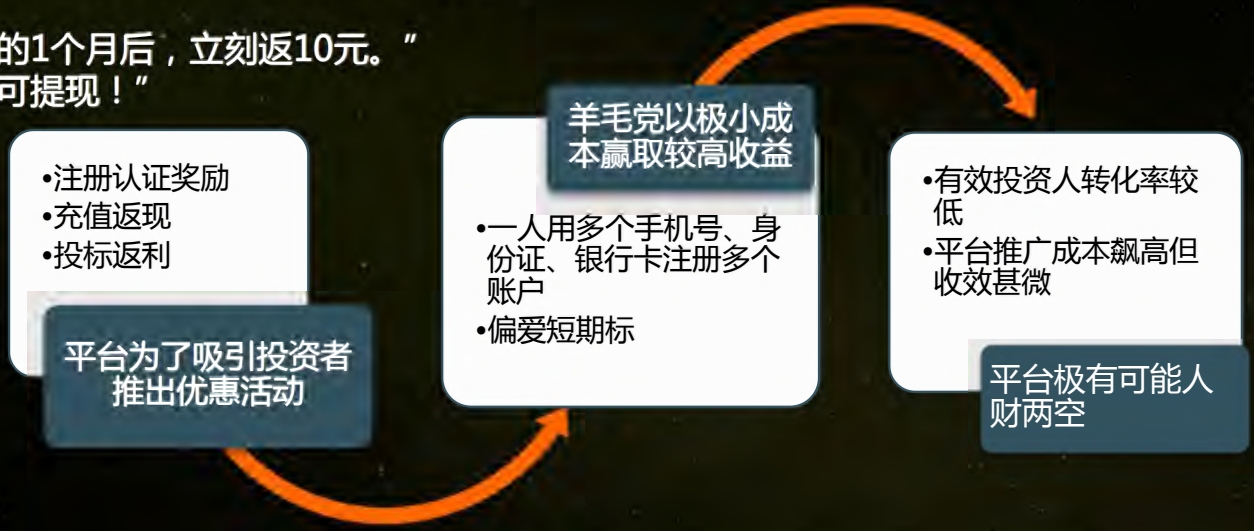
商户

1. 消费者难以判断优质商户
2. 商户的竞争变成恶意竞争
3. 电商平台的信用评价体系遭到破坏，长久下去对平台品牌形象造成严重破坏。

羊毛党骗取补贴（P2P、理财）

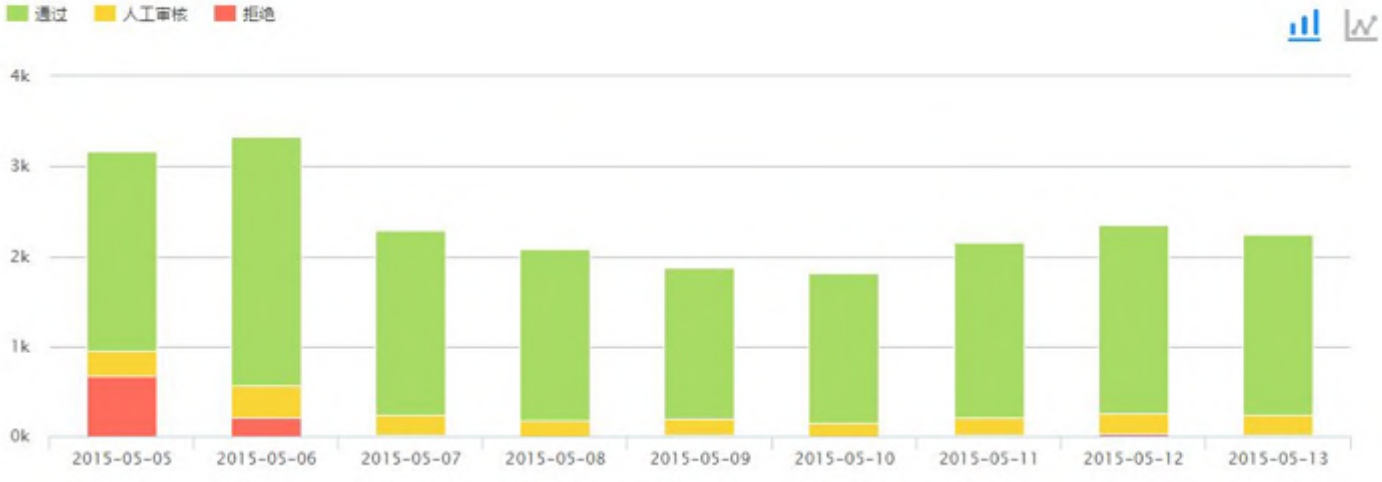
羊毛党——善于利用商家的优惠促销活动，以低成本或零成本赢取高收益的礼品奖品。

“充值50元，投资标的1个月后，立刻返10元。”
“注册即送20元现金可提现！”



羊毛党骗取补贴（P2P、理财）

同盾防垃圾注册解决方案、防羊毛党解决方案有效识别羊毛客



羊毛党骗取补贴（P2P、理财）

- 虚假手机号识别
- 通信小号识别
- 代理IP识别
- 设备指纹关联规则
- 设备欺诈历史查询

刷单骗取补贴（电商、O2O）

O2O平台

- 补贴用户：如新注册用户0.01元抢购电影票
- 补贴商家：商户评级、补贴返现

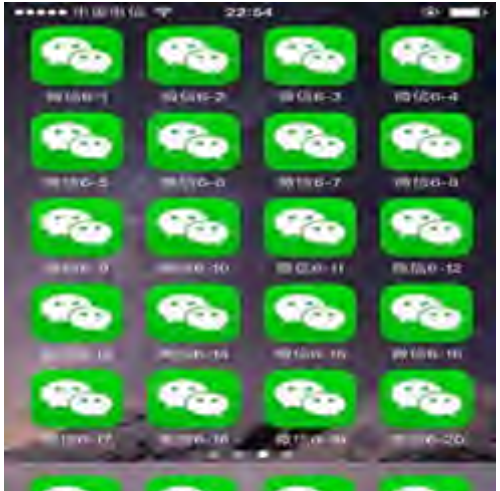
欺诈分子

- PC端手机模拟器
- 收码平台（提供虚假手机号用于注册）
- 虚拟定位（模拟地理位置）
- 代理IP、VPN

O2O平台

- 用户以近乎零成本骗取平台补贴
- 用户与商户合作刷信用、骗提成

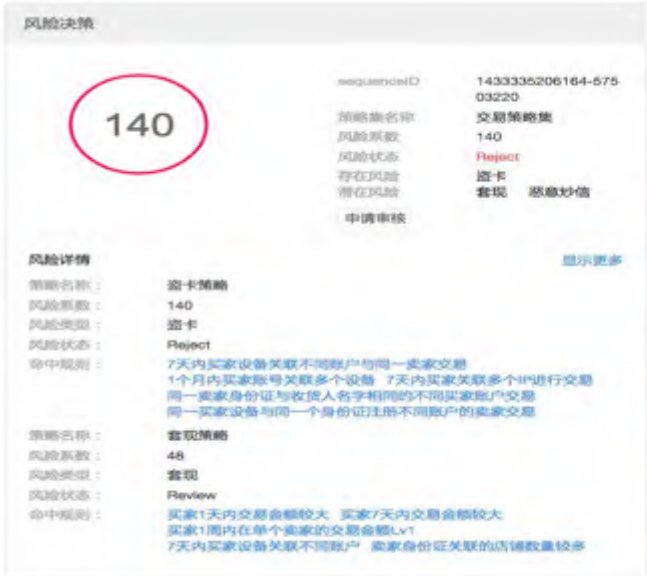
刷单骗取补贴作案手法（电商、020）

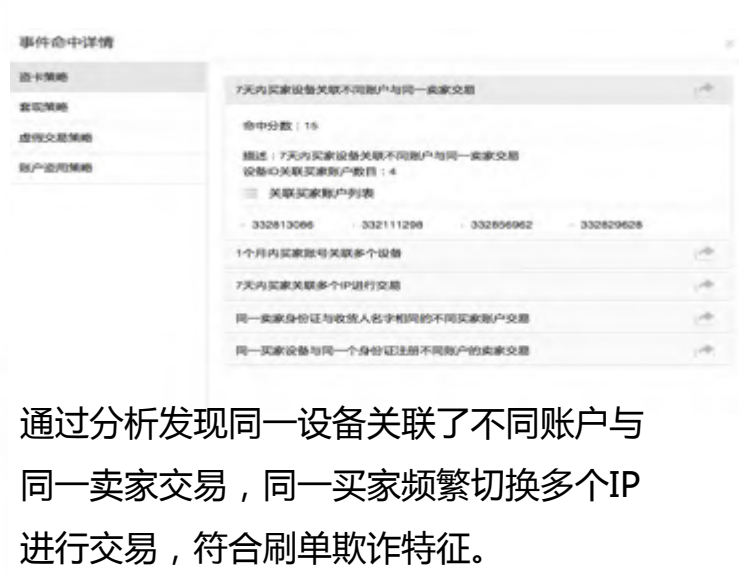


刷单骗取补贴（电商、O2O）

移动端设备指纹SDK	•稳定的设备ID •模拟器检测 •越狱检测
VPN检测 及多开检测	•VPN、SOCK4/SOCK5等多种代理方式 •真实IP识别 •检测同一设备安装同一应用的多个客户端刷单
刷单交易风控规则	•账户关联规则 •设备关联规则 •IP关联规则

刷单骗取补贴（电商、O2O）





通过分析发现同一设备关联了不同账户与同一卖家交易，同一买家频繁切换多个IP进行交易，符合刷单欺诈特征。

抢红包、秒杀（电商、O2O)

黄牛抢货的灰色利益链条

抢红包、秒杀（电商、O2O）

设备

秒杀软件

人机识别算法
设备id点击频度
时间相关规则
设备id关联账户
鼠标点击事件
页面停留时间
UA匹配
.....

同盾反欺诈规则模型

识别黄牛党

国内互联网行业反欺诈现状

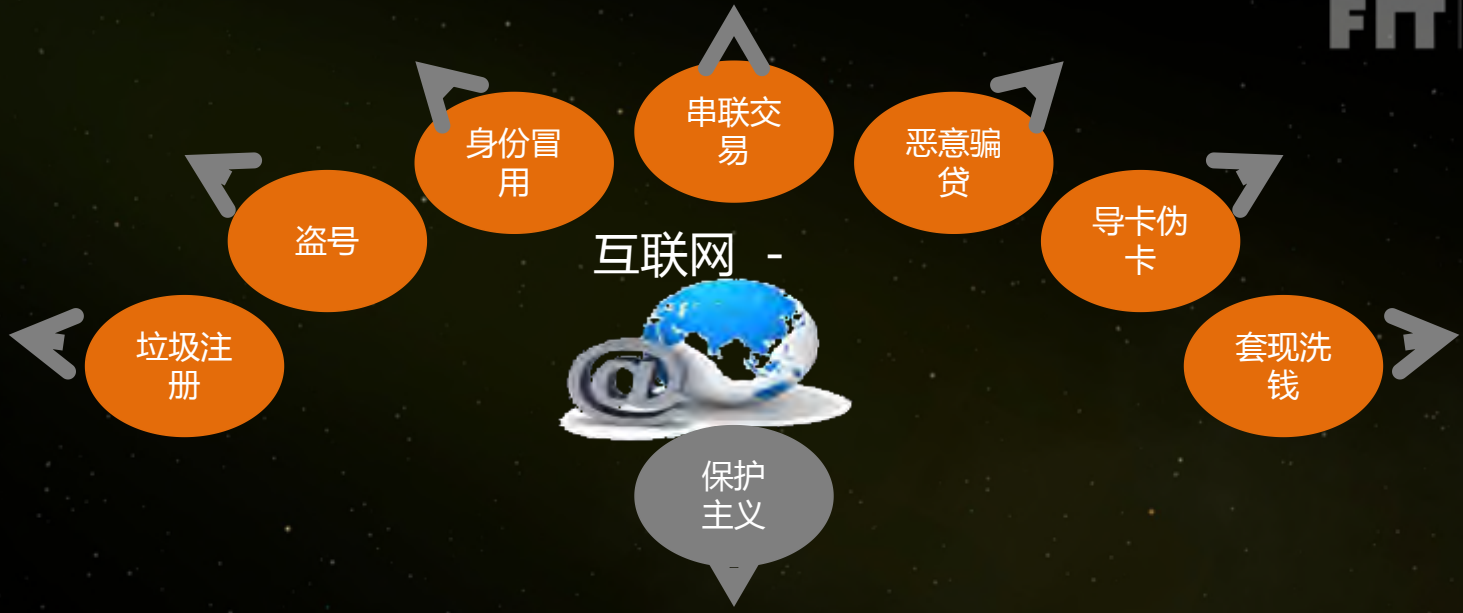
- 单兵作战，无联防联控
- 对线上欺诈风险认知不足
- 对交易以外的欺诈忽视（登陆，注册）

反欺诈3.0时代的到来

反欺诈1.0
- 简单可疑行为（透过惨痛教训获得，事后）
- 业务系统内嵌反欺诈（不灵活，效率低）

反欺诈2.0
- 业务系统 / 风控系统分割
- 单打独斗

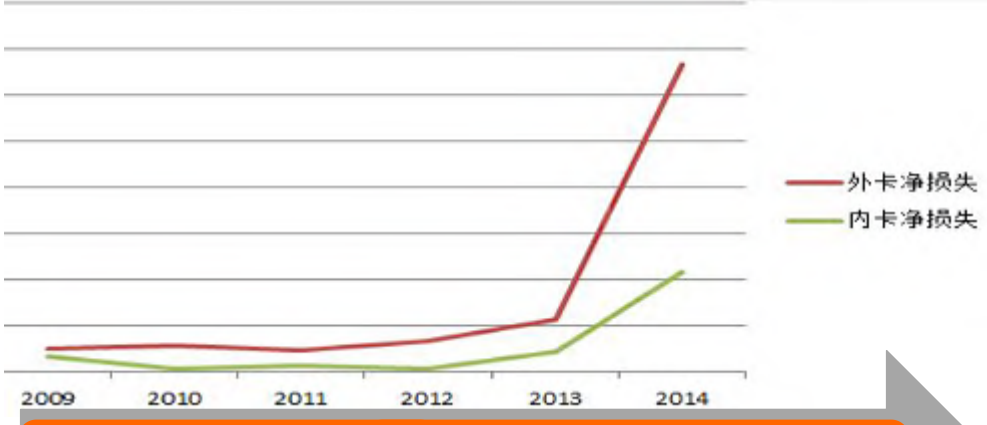
反欺诈3.0
- 大数据年代
- 聚焦诈骗分子



跨行业联防联控

有人就有江湖

携程最近几年风险事件发生趋势



个体作案，盗号，欺 木马，盗卡，盗号，欺诈，销
盗卡 赃产业一条龙

团伙化

地域化

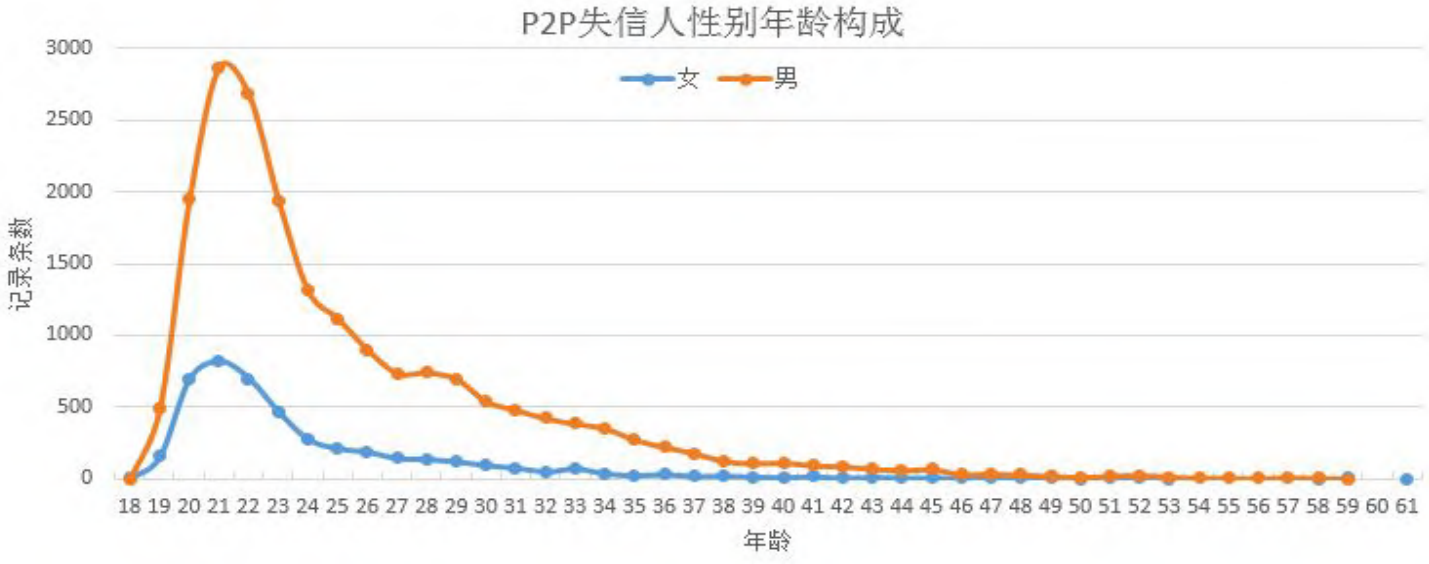
年轻化

专业化

团伙化、地域化


失信人出生地分布图
648
719
42
3075
526
655
660
2413
105
1453
753
972
926
8
661
119
958
1397
680
1437
792
555
845
314
659
981
307

年轻化


P2P失信人性别年龄构成
女
男
记录条数
3000
2500
2000
1500
1000
500
0
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61
年龄

专业化：风险领域的不公平对抗

专业化：风险领域的不公平对抗

黑色产业链
地下论坛
成熟的骇客工具

单一企业风险智能

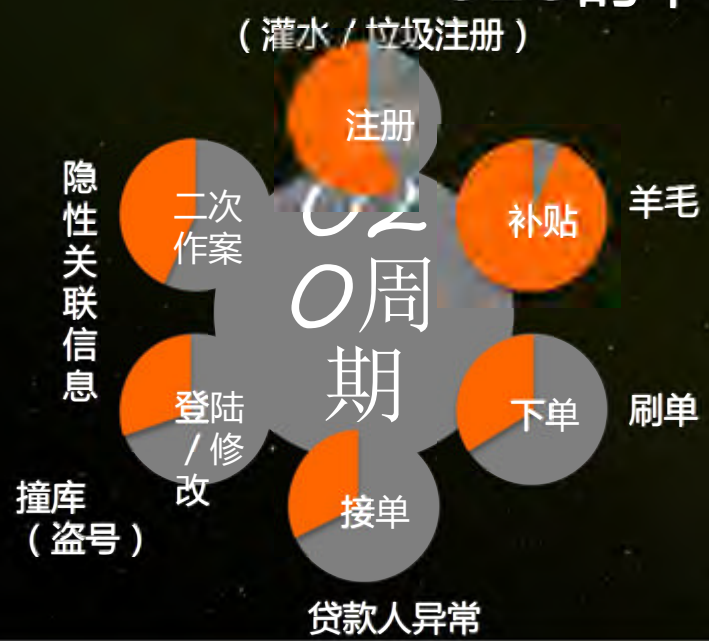
安全本该未雨绸缪
何不早日风雨同舟

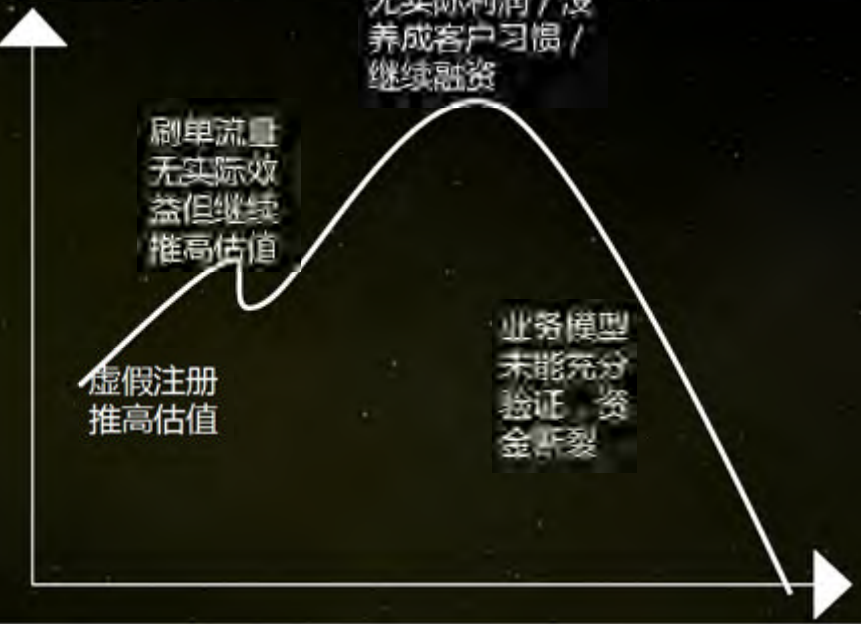
跨行业联防联控

同盾风控核心技术体系


高危账号
设备指纹
代理检测
指标计算
同盾
大数据反欺诈
技术体系
构建网络反欺诈云
跨行业联防联控
让欺诈无处遁形
风险引擎
失信名单
欺诈信息库
地理位置库

O2O的羊毛恶性循环


（灌水／垃圾注册）
注册
补贴
羊毛
下单
刷单
接单
贷款人异常
登陆／修改
二次作案
隐性关联信息
撞库（盗号）
O2O周期


无实际利润／没养成客户习惯／继续融资
刷单流量无实际效益但继续推高估值
虚假注册推高估值
业务模型未能充分验证，资金断裂

总结

大数据在下行经济的影响有利有弊，反欺诈是海啸前夕的一道防御堤坝

- 之前没有过可比的历史数据
- 普遍分析偏向依靠正面预期
- 八七美国股灾里崩盘的教训
- 判断负面数据会更显得重要
- 同盾负面画像防范诈骗井喷
- 对拐点中的信用市场很重要

同盾在的反欺诈领域的愿景

利用大数据技术下的反欺诈模型，服务支付平台的风险
（合作 / 共赢）

透过合作，把反欺诈服务

服务 领域拓展的新业务

家没有大数据病的专业反欺诈服务商

愿天下无贼

Jackal.ma@fraudmetrix.cn

www.tongdun.cn

杭州同盾科技有限公司
杭州 * 北京 * 上海 * 深圳

邮箱：mkt@fraudmetrix.cn

Thanks