



银行卡收单业务 风险形势分析及防控建议

北京 2018.05

目 录

CONTENT

01 当前收单业务风险形势

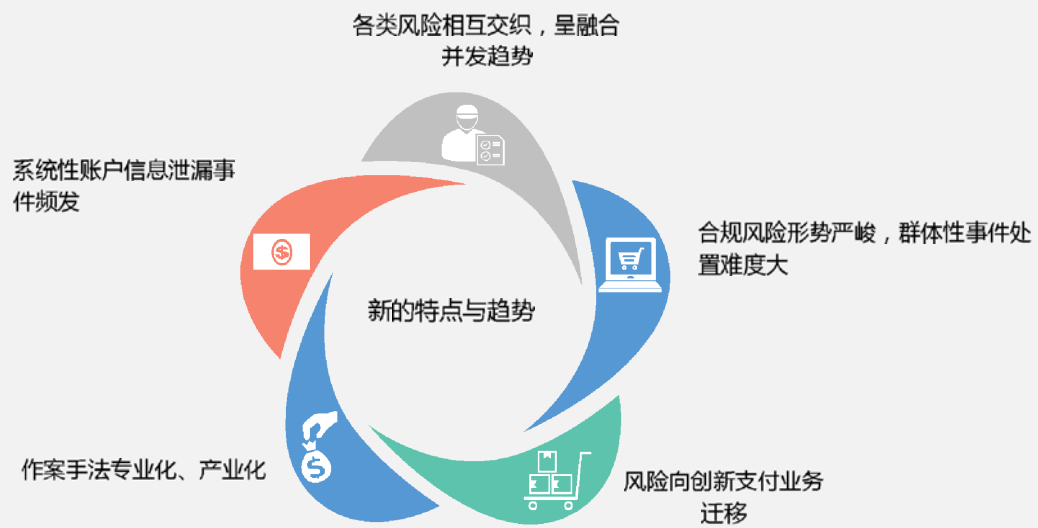
02 典型案例分析及防控建议



当前收单业务风险形势



当前收单业务风险形势





典型案例分析及防控建议



盗刷流程

集团化作案，分工明确，侧录-制卡-盗刷呈一条完整犯罪产业链





侧录案件的发展



自制
设备



专业
设备



个体
作案



犯罪
集团



无反侦测
意识



有反侦测
意识



侧录点的选择





创新业务欺诈案例主要特征

01

欺诈攻击呈现有组织、专业化、波段式特征。



02

欺诈交易集中于初始绑卡验证环节。



03

新型网络犯罪技术是实施作案的主要手段。



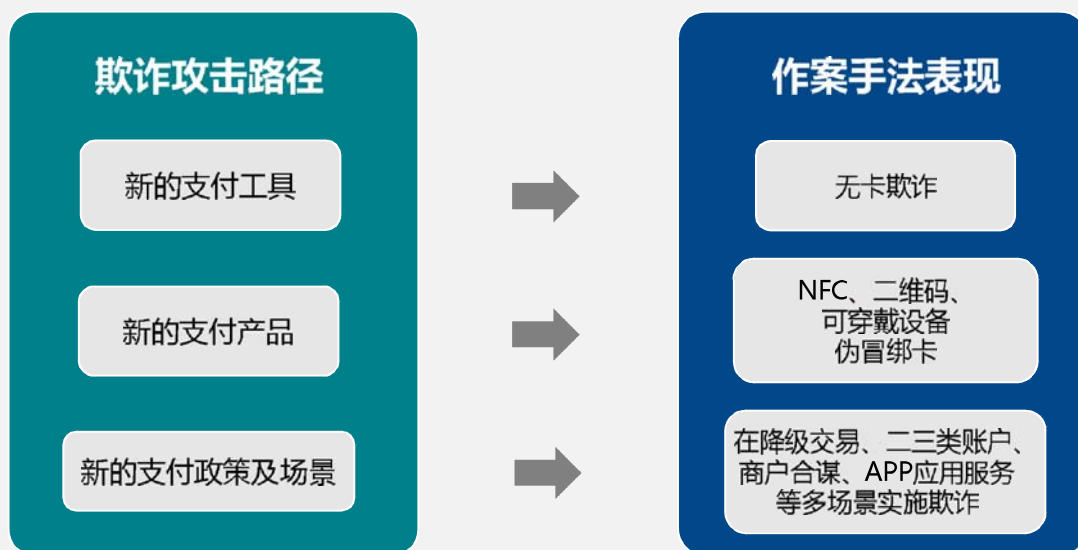
04

与线下商户勾结合谋成为实施欺诈的重要途径。





创新支付业务的欺诈表现形式



无卡案例



假冒客服退款诈骗



伪基站发送欺诈短信



篡改银行预留手机号

核心：获取短信验证码

虚假提额诈骗



利用社交工具诈骗



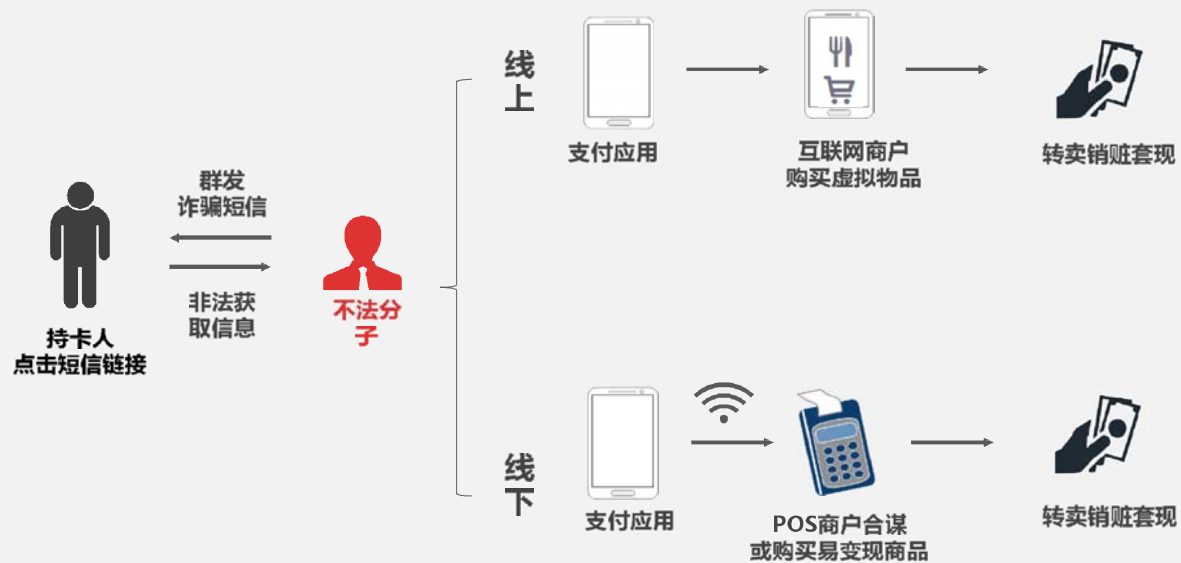
伪冒补办手机SIM卡



利用理财账户盗转资金

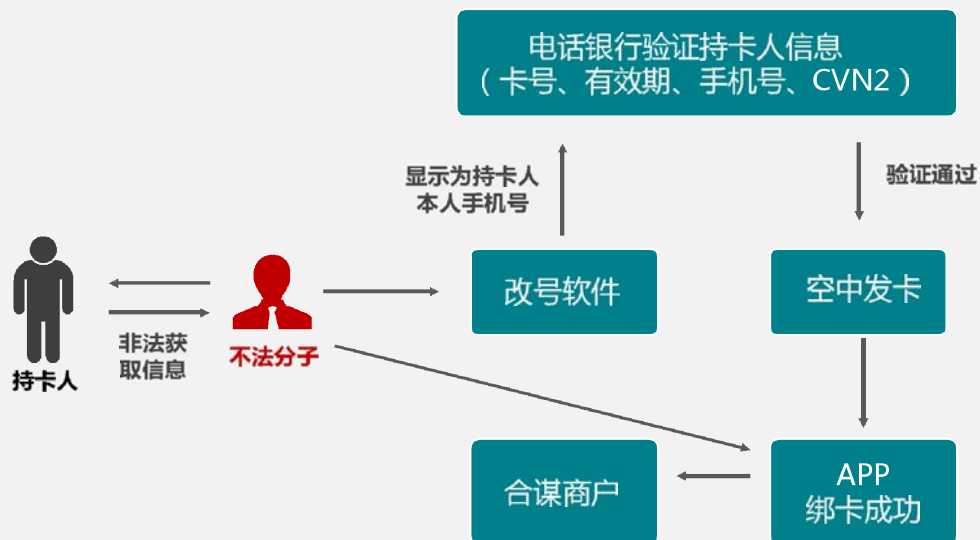


利用木马病毒伪装绑卡





利用改号软件伪冒绑卡





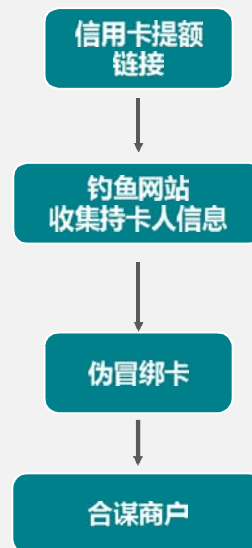
假冒信用卡提额伪冒绑卡

手机浏览器界面显示假冒信用卡提额伪冒绑卡页面。地址栏显示 <http://www.eitituo.com/3.html>。页面标题为“信用卡 CREDIT CARD”。

表单包含以下输入项：

- *有效期: 如01/17 填201701
- *cvv2后三位: 卡片背面签名栏后三位
- *手机号码: 银行预留手机号码
- *当前额度: 请输入当前额度
- *申请幅度: 请选择...
- *查询密码: 请输入6位查询密码
- *交易密码: 请输入6位交易密码

底部有手机浏览器的导航栏，包含返回、前进、主页、书签和菜单按钮。



□ 入网审批

人脸识别、设备指纹、定位技术、图像识别、网络爬虫

□ 事中控制

动态调整商户结算模式措施

对于部分创新业务，根据商户销售的实际商品类型设置不同规则、限额。

□ 监控及处置

重点监控：

✓ 新上线产品及业务

✓ 短时间内连续多笔交易、失败交易较多、休眠商户突发交易、异常大额交易、交易特征与商户交易场景不符等异常情况

一旦发现异常情况，应实地检查商户和终端机具的情况，及时采取暂停交易、延迟商户结算资金或撤机销户等措施。

套现的发展



商户
套现



个人
套现



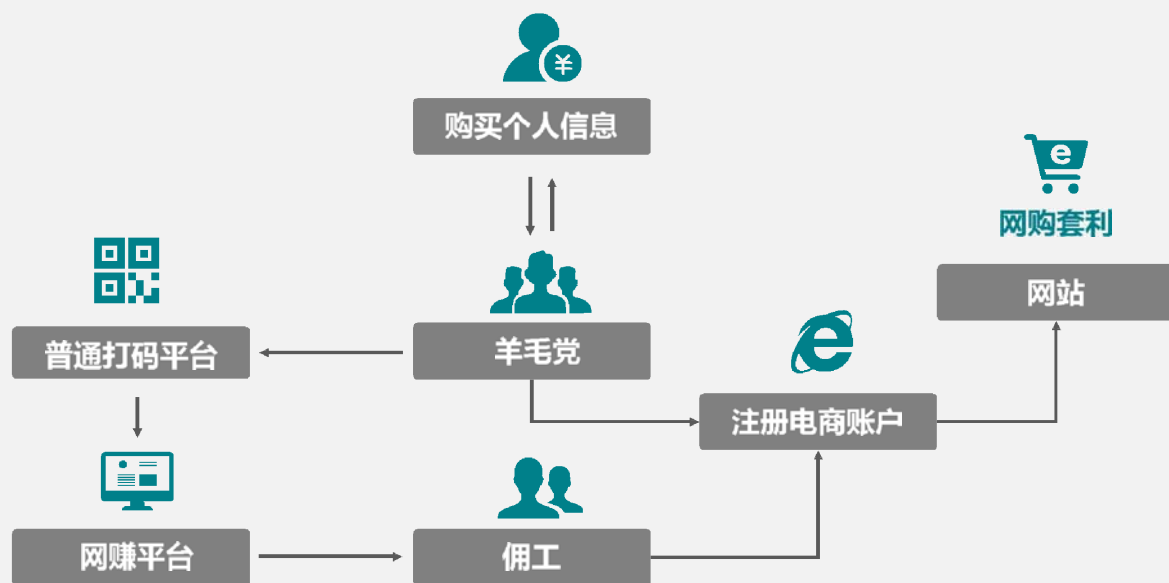
移动
互联网

- 建议全面梳理辖内存量线上商户（尤其是交易量大的重点商户）的交易场景、区分真实场景
- 如发现金额贴整数、笔均金额异常、贷记交易占比高等异常特征的商户，及时核实交易场景，排查是否直接或变相为持卡人提供套现服务，并采取相应防控措施





羊毛党产业链



羊毛党利益链条



03

防控建议

一是落实监管要求、加强合规经营，守住不发生系统性风险的底线。

积极宣贯《中国人民银行关于进一步加强银行卡风险管理的通知》（银发[2016]170号）、《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发〔2016〕261号）、《关于进一步加强无证经营支付业务整治工作的通知》（银办发〔2017〕217号）、《中国人民银行关于规范支付创新业务的通知》（银发[2017]281号）、《中国人民银行关于印发《条码支付业务规范（试行）》的通知》（银发[2017]296号）等监管政策要求，始终保持打击防范电信网络新型欺诈、账户信息泄漏、非法套现、无证经营支付业务等风险的高压态势，加强合规经营，配合人行、总公司做好相应工作，守住不发生系统性金融风险的底线。

二是强化异常交易监控，及时开展调查处置。

针对异常交易特征开展监控及调查处置，特别针对新上线产品及业务加强交易监控，一旦发现异常情况，应实地检查商户和终端机具的情况，及时采取暂停交易、延迟商户结算资金或撤机销户等措施。

三是加强联动处置，妥善处置群体性事件。

对于日常交易监控中发现的异常情况，及时报送银联，以便开展风险排查和后续处置。
对于银联发送的风险提示，第一时间排查情况、开展防控处置，并将防控结果及时反馈。
一旦发生群体性事件，妥善做好持卡人及商户的安抚处置工作，避免舆情风险。



风险防控“五位一体”服务

一、风险规则支持

- 收单机构商户管理风险规则
- 互联网风险管理规则

二、风险监控服务

- 实时与准实时交易监控
- POC与CPP商户侦测
- 黑名单管理与信息共享

三、风险事件处置

- 资金延迟结算及货物拦截
- 高风险商户责任转移
- 警银联动快速响应

四、风险增值服务

- ARM/URM
- 风险数据：水晶球、火眼、设备指纹

五、风险损失化解

- 风险补偿



产业联动

- 银行卡安全合作委员会
- 互联网金融支付安全联盟

谢谢
T h a n k s

