1. 交易欺诈风险场景说明

1.1. 盗卡

释义：欺诈份子利用银行身份验证机制的薄弱环节，盗用他人身份证信息、手机号码、银行卡账户等信息，假冒被害人身份进行欺诈交易。

表现形式：主要为持卡人在卡片未丢失、支付密码未告知他人的情况下、资金被完全陌生的第三方冒名消费、转账或提现。

风险来源包括：密码遗失、撞库信息泄露、钓鱼信息泄露、黑产购买等

风险特征包括：频繁交易，陌生设备，接近限额，变更手机号、限额，累计多笔接近余额，分散转入分散转出，登录成功，但交易密码错误N次，更换设备然后变更手机号（或新加手机号）向陌生收款人转账，长时间未交易后多笔大额集中转入、转出

特征分析：

规则建议：

1.2. 伪卡

释义：多指欺诈份子通过其技术手段复制出原卡信息进行违法刷卡套现的卡。

表现形式：为非芯片信用卡侧录，一般行的信用卡是靠卡片上的磁条记录持卡人的资料代码，另加一组识别码。如果与刷卡机连线，或是用一台有记忆储存设备的读卡机(侧录器)，将信用卡在上面刷一下，就可以将真卡的数字全部记录下来。欺诈份子取得这些数字后，用空白的卡片(俗称白卡)贴上磁条，输入侧录的代码，再用凸字机打出，打印防伪标签，这样就做出了一张与发卡银行所发的信用卡相同的假卡。持假卡消费的人，通常在被发现或被停卡之前，会连续大量刷卡消费，直到刷爆为止。

风险来源：

1）因银行过错导致持卡人信息（银行卡号、密码等）被违法行为人或犯罪嫌疑人截获，例如在ATM机周围安装摄像头等设备盗取信息、在ATM机上安装吞

卡装置、盗取真卡内资金；

2）因持卡人自身的过错导致银行卡信息泄漏，比如银行卡丢失、密码泄露等持卡人未妥善尽责的履行保管义务；

3）是银行卡信息泄漏原因不明，如黑客侵入系统盗取持卡人信息来制作伪卡。

风险特征：通过非法手段获取持卡人信息，并根据所获得的信息制作伪卡，然后通过自动取款机（ATM）或多功能支付端（POS、EPOS）在本地、境内异地或境外，盗刷卡内资金。其他特征还有敏感时间、高危地区短时高频、频繁大额交易，异地交易，流量异常波动，幅度过大，挂失卡交易等

1.3. 套现

释义：一般是指用违法或虚假的手段交换取得现金利益。表现形式集中在信用卡套现、公积金套现、证券套现等，套现多会考虑免息周期，一般是 20-56 天不等

表现形式：套现多表现为使用销售点终端机具（POS）等方法，以虚构交易、虚开价格、现金退货等方式向持卡人直接支付现金；或者商户与不良持卡人或其他第三方勾结，或商户自身以虚拟交易套取现金，套现一般需要收取 1.5-3%不等的手续费，空卡套现手续费用则为 15%-25%不等。另外还存在翻倍套现，即借助于分期付款额度，先分期付款一次，将分期额度用完，然后直接一次性刷卡一次将信用卡额度内的可用额度消费完，这样就可以消费分期额度+信用卡额度内可用额度的金额，实现信用卡翻倍套现。

风险来源：1）持卡人的个人行为 2）持卡人与商家或某些“贷款公司”、“中介公司”合作，持卡人通过付给商家手续费来获取套现。一般是利用商家的 POS 机进行虚假交易。3）持卡人利用一些网站、公司或者第三方支付平台的服务而取得套现 4）小额免手续费套现

风险特征：敏感时间高频或大额提现，贷记卡次数或金额累计占比过高、幅度过大，异常地区，虚假商户，金额异常，关联外部中介、第三方支付等

1.4. 洗钱

释义：是指将走私犯罪、黑社会性质的组织犯罪、卖淫犯罪、贩毒犯罪或者其他犯罪的违法所得及其产生的收益，通过金融机构以各种手段掩饰、隐瞒资金的来源和性质，使其在形式上合法化的行为，这些犯罪活动主要包括：赌博、传销、贩毒、走私、诈骗、贪污、贿赂、逃税等

表现形式：洗钱行为一般具有方式多样、过程复杂、对象特定及国际化等特征。可归类如下

1.现金走私；

2.集中转入后再将大额现金分散存入银行；

3.向现金流量高的行业投资；

4.购置流动性较强的商品；

5.匿名存款或购买不记名有价金融证券；

6.制造显失公平的进出口贸易；

7.注册皮包公司，虚拟贸易；

8.设立外资公司；

9.利用地下钱庄和民间借贷转移犯罪收入；

10.购买保险；

11.实施复杂的金融交易；

12.在离岸金融中心设立匿名账户；

13.利用银行保密法洗钱。

风险特征：敏感时间、异常群体、异地、大额、多笔高频、突增、黑/灰名单、集中转入/分散转出、异常金额、跨境、单一账户关联大量对方账户等。

1.5. 扫码

释义：一般指欺诈份子利用各种技术手段，攻击被害人所使用的电子交易终端，劫持会话或植入木马程序等恶意代码，直接操纵交易终端进行二维码替换。

表现形式：通过手机、微信等平台发布虚假信息，诱使当事人扫描后可进入正式流程。而此二维码则为伪冒二维支付码，一旦扫描，手机 APP、微信钱包中

的金额就被自动刷走。

风险来源：木马、钓鱼网站、虚假链接

风险特征：非常用基站、地区，设备异常，异常地区，修改关联设备，模拟机识别等。

1.6. 薅羊毛

释义：泛指搜集各个银行等金融机构及各类商家的营销优惠信息后，利用积分、抵扣券、打折券、代金券、红包、红利等进行资金赚取的行为称之为薅羊毛。

“羊毛党”则是指用利用各商家的优惠促销活动，以较少的成本或零成本赢取相对较高收益和奖品礼品的群体。目前一些理财平台注册即送现金红包，由于羊毛党通过大量的垃圾注册多次在同一平台获取营销红利，使得平台在市场推广上的效果欠佳。

表现形式：多为羊毛党批量注册用户，并领取实物、优惠券、返现券等。批量注册行为一般伴随代理 IP 的切换，但设备可能不会变化。所以可以基于设备指纹进行设备识别，对同一设备注册账号、参与活动次数进行聚合统计，也可统计短时间多维度频度等

风险来源：互联网黑产、羊毛党等

风险特征：信息雷同，非习惯，相同设备高频，虚拟设备环境、代理访问，频次及时间跨度含设备、IP，关联维度异常，短时间内大量且快速交易，批量注册、签约、绑卡，积分兑换，异常行为，代理点虚增交易量套取手续费等。