电信诈骗案例：

网络电信诈骗，卡内资金被骗

- 某行大量老年人社保金账户被不法分子利用，资金被快速转移。

案件调查：利用线下促销或者网络活动，登记老年人身份及银行卡信息，进行资金诈骗。

案件特征：

诈骗分子养号，长期保留一些银行活跃账号，先进行一笔小额试探，然后进行大额资金行内账户转入，再快速非同名跨行转出。

采取措施部署规则：

部署规则组，含六个条件：

1、当日有 10 元以下小额资金转出。
2、当日有一笔以上大额资金（大于等于 5000 元）转入。
3、当日有一笔以上大额资金（大于等于 5000 元）转出。
4、当日转出资金与转入资金之差在正负 100 元以内。
5、大额资金转入转出时间在 2 个小时以内。
6、资金转出账户、被监控账户、转入资金账户，均非同一户名

薅羊毛、小额多笔、洗钱案件

盗刷、洗钱等

- 某行快捷支付渠道上，部分商户出现薅羊毛或者洗钱案件。

案件调查：利用下订单或者限额的规则，进行批量交易，或者多商户转账来进行资金归集后再分批消费交易。

案件特征：

单日或短时间虚拟商品（充值等）高频交易，集中转入后分散转出

采取措施部署规则：

按商品属性加限额规则
短时间或者当日累计次数规则
非同名多账户转入，多账户转出规则
同卡 bin 或者类似手机号高频交易规则

积分兑换案例：

收到积分换现金短信，卡内资金被盗用

- 客户收到一条显示为银行客户号码发来的积分兑换现金短信，并附有网址。点入该网址后按提示先后输入身份信息、银行卡信息和密码。但之后，其卡片即发生盗用。

案件调查：利用网络改号技术冒充移动公司或银行，并通过“伪基站”群发诈骗短信。短信中的网址为钓鱼网站并带有木马程序，以此获取用户银行卡信息并控制用户手机以窃取短信验证码。

案件特征：

交易商户为一游戏充值商户，因其同时经营实物产品，限额设置较高，致使该卡后续发生了近百笔的小额盗用。

采取措施部署规则：

按商品属性区分商户号并设置合理限额规则
交易习惯行为特征规则
地理位置的变化等风险要素辅助判断

篡改银行预留手机号案件：

篡改银行手机号至存款被盗

- 某行持卡人反映其名下两张借记卡被修改了预留手机号后，后被盗刷了两笔近 30 万元。

案件调查：主要是因银行手机客户端验证环节较薄弱，修改手机号时仅验证卡号、密码及原手机号，使欺诈分子在掌握相关信息后篡改了其预留手机号并用以接收盗用支付的短信验证码。而发生欺诈的商户为以纸业公司为名虚假注册商户，因收单机构入网时未严格审核其资质，且设置了过高的限额，商户仅入网两天即发生了大额欺诈。

案件特征：

各类信息泄露事件使得欺诈分子能低成本地掌握大量用户信息，并通过撞库等手段进一步获得密码等敏感信息。而部分银行对预留手机的管理存在漏洞导致持卡人手机号被篡改的情况时有发生。

修改关键操作后进行大额或者高频交易。

采取措施部署规则：

修改关键操作后进行大额或者高频交易；

增加虚假手机号码库和通信小号识别库，用以识别手机号码的欺诈风险。

快捷支付的风险案例：

- 客户来电表示其手机收到 10 笔快捷支付的扣款短信，金额均为几十元，非本人操作，需要核实。
- 客户致电其借记卡在 11 月 7 日 16：50 进行了一笔 5 万的快捷支付，并不是自己操作的，需要核实。
- 客户 11 月 07 日来电反映，发现有一笔 139 元网上虚拟产品支付交易，但记不得这笔交易是自己做的，需要核实。

…… ……

案件调查：不法分子通过欺诈手段，诱使客户开卡并在银行预留不法分子提供的手机号，然后在客户不知情情况下绑定快捷支付，并购买点卡、充值卡等便于销赃洗钱的虚拟商品。

案件特征：

交易设备不是客户习惯使用的设备；

交易 IP 地址不在客户开户行所在地区；

开卡不久（2-3 日内）就被盗；

签约手机号属地不在客户开户行所在地区；

购买商品多为虚拟商品，如点卡、充值卡等。

采取措施部署规则：

开卡 N 日内发生快捷支付交易；

签约手机号属地不在客户开户行所在地区；

接近限额的快捷支付大额交易。

利用理财账户转移盗刷资金典型案件：

银行卡资金被盗转，某行持卡人报案称其卡内 13 万元资金被人盗用转入了某基金账户，并后续被人转至其他银行卡中。后经警方查明，欺诈分子通过 QQ 群购买到了卡主身份信息及银行卡信息，并通过伪造的临时身份证以陈先生名义办了新的同名卡。而后其盗用陈先生银行卡购买基金并在换绑新卡后赎回。而这

其中，基金公司在首次绑卡及换绑中仅验证了卡号、姓名、身份证号，未验证卡密或手机号及短信验证码。

案件调查：利用理财账户盗转资金近来欺诈尝试明显上升，而个别基金商户因业务中存在的漏洞，被欺诈分子利从而盗走资金形成损失。这不仅是因为个人信息存在泄露情况，更主要的原因是在商户绑卡验证、换绑策略、资金闭环等方面的漏洞所导致。

案件特征：

绑卡后短时间内进行交易；

购买基金尝试频繁且金额较大。

采取措施部署规则：

签约或者绑卡后金额大额或者高频交易；

接近限额大额交易。

欺诈案例 1（手机银行）：

2016 年 6 月 5 日，泉州发生客户卡内大额资金被他人通过手机银行分别转账 49.99 万、29.99 万元事件。

欺诈特征分析：

- 手机银行大额转账
- 首次收款人
- 签约手机号不是预留手机
- 当日大额转进转出

……

监控规则：

手机银行大额转账监控规则经过测试后，6 月 10 日部署上线。当日即发现一笔欺诈交易。随后将欺诈交易设备号、手机号加入黑名单。

欺诈交易拦截：

监控人员发现黑名单设备登录手机银行并发起转账 29.99 万元情况，立即联系客户本人，提示风险，阻断不法分子实施诈骗，及时避免客户资金损失。

某行风险监控中心连续多日每日发生“卡一日内累计取款次数超过 5 次”的预警。经查询，这些取款动作均发生在每日凌晨 1 点钟开始到清晨 7 点钟左右，为有两个外行银行卡在同一个 ATM 机频繁取款，每次取款 100 元和 200 元，基本每隔 10 分钟轮流发生一次取款交易。

连续多日敏感时间发生多笔交易

复制银行卡

客户敏感信息泄漏

欺诈案例 2（快捷支付）：

某行一客户在淘宝上购买商品并且付款成功，犯罪嫌疑人冒充支付宝客服人员，谎称付款系统正在升级，要帮客户退款，要客户提供卡号、身份证号、支付宝支付密码和手机验证码。

风险分析：

这是一种新型的电子支付风险，不法分子利用客户不甚了解业务，在客户不明真相情况下，不法分子“帮”客户开通快捷支付，造成了资金损失。

监控应对策略：

1、签约快捷支付后即刻支付，达到付款限额的90%以上。

2、签约快捷支付后，即刻修改绑定账户所签约账户信息即时通手机号。

3、付款交易失败，系统报错“账户余额不足”。

欺诈案例3（网络钓鱼）2015年12月一客户下订单后，选择通过支付宝支付。在支付过程中订单被修改为金额相同的订单到汇付天下。

风险分析：

订单中商户信息被篡改，客户不明真相情况下自己操作付款造成损失，而且金额一般不大，难以适用群体性规则，可设置个人行为习惯规则，防范此类风险。

监控策略：

1、客户非习惯使用的第三方支付平台（统计数据显示，人均使用的支付平台为1.3个）。

2、客户非习惯支付类别（一般修改后的订单通常支付类别为游戏点卡等）。

3、达到客户网上支付交易限额的90%以上。

欺诈案例4（信用卡违规操作）

2016年7月，支行信用卡业务员，用一个手机号做了账户预留手机号码，办理了几百张信用卡，被系统监控预警。经核实为柜员违规操作，同一时间批量开通了600个网银账户，从中谋取私利。

欺诈案例5（网络诈骗）

犯罪嫌疑人佯装与受害人签订合同，骗其在借记卡中存入现金10万元，在受害人电脑中植入木马，盗取其交易密码，骗其登录网银，远程操作转走客户资金，再将资金转向他行或直接ATM取现。

风险模型分析：

特点是客户新开卡后1至2日内存入大额现金，或新开网银当日，通过网银转账转至他人账户，然后再将资金转向他行或直接ATM取现，大多使用网银互联汇路（实时到账）。

监控策略：

1、新开卡2日内发生大额网银转账（同行），转入账户短时间内再次转出。

2、新开卡2日内通过网银互联汇路发生连续N次大额跨行转账，其中单笔转账金额接近5万（如大于等于4.5万）。

3、新开网银，当日发生大额跨行网银转账。

4、新开网银当日通过网银互联汇路发生连续N次大额跨行转账，其中单笔转账金额接近5万（如大于等于4.5万）。

5、辅助规则：上调网银转账交易限额；修改账户信息即时通签约手机号；网银转账交易IP与账户机构分属于不同城市；账户余额少于转账金额。

ATM、POS自助渠道风险

案例：2014年6月，连续多日每日发生“一日内累计取款次数超过5次”的预警。经查询，这些取款动作均发生在每日凌晨1点钟开始到清晨7点钟左右，为有两个外行银行卡在同一个ATM机频繁取款，每次取款100元和200元，基本每隔10分钟轮流发生一次取款交易。

调用ATM监控录像查看，发现在此时间段并没有人在ATM上有取款动作。经ATM客户端操作日志与服务器端ATM交易记录比对检查，初步确定此ATM

机 C 端程序存在问题，对此 ATM 机业务部门立即进行了封存，进行故障原因调查，并且对账务错误对兄弟单位进行了通报。

另一场景介绍：

广东银监局下发了《关于加强和改进银行卡管理工作的通知》(广州银发[2012]64)，要求各发卡银行要加快行内系统改造，完善持卡人各项登记信息，包括手机号码、联系地址、紧急联系电话等，并于 2012 年 11 月 30 日前开通免费向持卡人提供余额查询的短信提醒服务

实现方式：

1、自助渠道应用（包括 ATM、POS、银联前置、查询机）收到客户的查询请求后，按照交易监控的报文要求将查询交易信息发送监控系统。

2、通过监控系统管理端配置规则“账号开户行所属分行为广东地区分行”，满足该规则的交易将按照短信通知流程处理，调用短信平台发送通知短信。

业务量统计：

目前该业务覆盖了广东地区开卡的客户，统计数据显示，目前监控系统每天收到全行自助渠道查询交易 20 多万笔，向广东地区客户发送短信大约 2 万笔左右。

ATM、POS、手机银行渠道自上线以来，日均分析各渠道交易（含登录）笔数 600 余万笔/日，三个月时间已累计监测风险交易 20000 多笔，识别并预警高风险欺诈交易 150 多笔，冻结资金账户 2 笔，系统在电子银行反欺诈风险其他渠道防控中已经显现出重要价值。

其他典型案例

2013 年 11 月，徽商银行数笔大额转账交易发生预警，预警内容为“个人金额 20 万元以上的单笔转账支付”、“三日内对私账户累积 100 万以上转账”以及“账户 10 日内资金分散转入、集中转出或集中转入、分散转出并且金额超过 20 万(个人)或者金额超过 100 万(对公)”，预警级别为橙色预警，三条预警同时触发。

调查发现在短时间内从某 3 人个人账户上发生转出交易 22 笔，每笔均为 50 万元，集中转出资金共计 1015 万元，转入账户 12 户。同时还发现该三人集中开立活期存单 22 笔，每笔 500 元。根据《中华人民共和国反洗钱法》，结合长期的经验积累和认真细致的分析，检查人员认定这是一起大额可疑交易，并于同月 23 日向公安局经侦支队进行了报告。

经有关部门调查和侦破，初步确认，本次预警与一起涉嫌有预谋的诈骗案有关，作案者化整为零，自以为手法高明，最终在“电子眼”—风险实时预警系统的监视下，还是漏出了马脚，避免重大案件的发生。