**支付公司如何预防和治理重复出款的风险**

**瀚银支付**

保障客户备付金资金安全是每个支付公司的首要职责，所以人民银行也下达了一系列措施和规定，需要支付公司严格遵守《支付机构客户备付金存管办法》。需要支付机构和备付金银行能够逐日逐笔核对客户备付金交易明细，支付机构的公司治理规范、风险管理制度健全、客户备付金安全保障措施有效。

支付机构每月人工和备付金银行核对数据，并每季度需要在人行的客户备付金信息核验系统内进行上报以下信息：

1，支付机构与各备付金银行分别就其业务系统中记载的当期出入金业务与备付金银行账户出入金信息进行核对、校验。

2，支付机构与备付金存管银行法人（或其授权分支机构）就支付机构业务系统中客户资金账户当期发生额、期末余额与全部备付金银行存款的变动及余额进行计算和核对。

但所有支付系统都是人开发的，难免会有出错的时候，那我们如何来保障支付机构不发生重复出款，我来简单谈下预防和治理的方法。

**一般的出错场景**：

1. 程序逻辑错误

每次出款，都等银行返回结果后，再去保存数据库出款成功的结果。一旦网络异常或者数据库繁忙，无法插入成功状态或者其他原因导致存储过程回滚，这时候由于最终状态没有更新，所以能够重复再次出款。

1. 隔日场景，或者服务器时间差

某一笔结算流水，刚好跨天了，比如23：59分提交，银行出款在下一天。但因为未能正常异步通知成功，查询程序却去查询昨日有无成功，没有结果，则导致再次出款。有时候由于上游服务器和你生产服务器时间差几分钟，也会导致查询失败再次出款。

1. 多个定时任务

一般定时任务跟随项目工程文件一起提交，容易被部署在多台服务器集群内，当代付的Job在多台服务器上运行时，那必然会导致重复出款。

1. 服务器异常崩溃

服务器异常崩溃、如果是windows server还会发生蓝屏等，导致没法完成数据库的存储，异步通知的发送，甚至redis内存状态的丢失等，都会可能导致重复出款。

1. 提交并发

一般是财务审核的按钮提交并发，或者自动审核的话，提交的时候产生并发，就会导致重复多次出款。

**作为支付机构，主要需要保障以下情况资金安全**：

1，保障结算到结算账户不重复（T1，T0，D0）

2，保障结算到银行账户或卡不重复（T1，T0，D0）

3，保障商户（结算账户）结算款提现不重复

4，保障客户（支付账户）提现不重复

5，保障代付业务不重复

按重要度分（由重要—>次要）：

1. 代付业务不重复（因为批量业务，一旦一个批次重复，损失金额巨大）
2. 直接结算到银行账户或卡不重复（T1，T0，D0）（因为商户结算资金一般都比较大）
3. 客户提现不重复、商户结算款提现不重复（一般是单笔提现）
4. 结算到账户不重复（一般对账能否发现，可以发起冲正交易，避免损失）

**解决思路：**

一）把出款和结算，分步骤进行：

1. 把备付金出款分步骤： 1）生成出款批次 2）审核 3）出款
2. 把商户结算分步骤： 1）生成商户结算单 2）审核 3）出款
3. 把客户提现分步骤： 1）生成提现记录 2）审核 3）出款

二）各步骤增加风控机制

1. 生成代付批次时，先扣除商户余额，再处理其他；生成提现申请时，先扣商户余额或者支付账户余额，再处理其他。
2. 每一次代付请求或者提现，都需要通过一次财务审核（当两个批次，相同金额要出款，财务一般都能看出来），如果是D0、或者系统定时的T0，T1，系统也要自动做次审核动作。
3. 代付出款时，Job只处理已审核未出款的批次，但一旦进入Job，不管后续如何执行，都先标记“处理中“。所以哪怕这个批次再次进入出款队列，或者存储过程回滚，也不会再次触发重复出款。
4. 客户提现，均分批定时处理。渠道只有单笔接口，也封装成批量接口。（分批处理还能减少压力，减少单个重复的可能性）
5. 在生成结算单时，如果是T1商户，则一天只能生成一笔结算记录，时间范围就是T日。如果是T0商户，则看T0的场次，如果频次也是1天一次，那也只能生成一次结算记录。如果T0的场次是2次及以上，则严格根据交易时间来划分多个结算记录，保证各时间段不能重叠和重复生成记录。如果是D0商户，则每一笔结算记录生成，都要严格匹配交易记录。
6. 为了减少出错，系统自动处理的结算，都是严格按照D0，T0，T1的结算时间来处理，不会结算之前的交易。如果之前商户有资金未结算，则必须人工审核才能增加到出款队列。
7. 财务人工审核完毕，标记已审核，或者D0进入Job，立即标记为已审核。审核完毕，会标记为“已审核出款处理中”状态，等待出款。这里可以加一个风控，可以判断同一天内同一个商户同一结算金额不允许有多个结算记录通过审核，或者抛到结算异常中，等待财务人工再次确认。
8. 出款只保留4个状态：处理中，成功，已退回，异常。处理中、已退回和成功的出款，无法修改任何状态，只有“异常“状态的，可以人工再次出款或者标记为”已退回“。除了明确的”成功“标记，其他任何异常返回码对应的都是异常，这是为了防止上游渠道增加返回码，导致重复出款。所有的异常都抛到异常菜单，由财务人工后续处理。
9. 对于存在于异常的订单，1小时内由专门的查询服务器进行查询，财务人工只能处理1小时后的订单（系统人为锁定1小时，主要防止1小时内渠道变交易成功），如果想优化这个等待时间的话，建议把收款人信息错误的那些失败，单独筛选出来，可以让财务或者自动退回。
10. 在前端、后台都用上防重复提交的校验，杜绝提交并发的产生，可以参考以下链接：

<https://blog.csdn.net/Huozhiwu_11/article/details/78742886>  
https://blog.csdn.net/hikeboy/article/details/69789863  
一般就是1，禁掉提交按钮 2，在数据库中加约束 3，redis加锁 4，提交表单内生成一个令牌，服务器校验

11，出款需要接入人行规定的电信防诈骗前置机和建议接入过滤下银联的黑名单库。

* + 1. 增加系统和财务人工核账步骤

1. 【系统自动+财务人工复核】支付公司需要做到每日进行备付金自动校验，至少隔日能够发现系统是否发生了异常。我们大约花了3个月做了备付金自动校验系统。
2. 【系统自动校验】对于D0结算到银行卡，可以检测出款记录中是否已经存在该笔订单号；
3. 【系统自动校验】对于普通商户结算到账户余额，可以检测收支记录中，是否一天内有多笔相同金额入账，结算金额和前日交易金额是否匹配等。
4. 【财务人工复核】财务每天至少核对3次各备付金银行出款情况，与系统出款记录进行比对。
5. 对于异常单，财务处理时，必须先核对对账文件后，才能进行再次出款或者退回操作。（网联一般2小时，银联实时获取，部分直连银行需要隔日）。如果当日得不到退款对账文件的，一般建议隔日再给客户退款或者再次出款。
   * 1. 其他一些规则
6. 规定23:50-0:10分之间不能出款，以避免代付服务器与上游服务器有时间差，从而导 致无法准确查询得到出款指令。也避免有些银行隔日原因导致重复出款。
7. 相同定时任务只在一台服务器上执行，一旦服务器挂掉，就在另外一台人工起，不允许自动在多台服务器上开启定时任务。
8. 定时自动检查已审核，但实际未成功出款的订单。因为程序异常，蓝屏，数据库停止响应而没有出款的记录，都会以“已审核，处理中“的状态存在，而不是重复出款。虽然这个检查跟重复出款没有关系，但为了增加客户体验，建议这么做。

**控制出款风险的总原则：**

1. 先扣款，再生成处理订单，宁可长款也不能短款，宽进严出。
2. 自动校验商户的结算记录和客户出款记录，不允许同一天同一金额的结算记录产生多条。

如果同一客户相同金额的多笔出款，建议列入异常，由人工复核。

1. 只要进入处理流程，先标记“处理中”，对于“处理中”的订单，不能再重复自动发起
2. 除了成功之外，所有的其他通知的，都列为异常，需要人工处理
3. 异常的交易，需要定时器主动查询1小时后，再放给财务重新处理出款
4. 需要有一套系统自动备付金校验系统，每日深夜自动与备付金银行核对，并次日财务人工确认。
5. 不允许同一付款的定时器在多台服务器开启。
6. 出款跳过23：50-0：10这一时间段，避免上游服务器和你服务器之间的时间差，产生隔日出款。
7. 审核提交等，加上前后端的防并发处理，防范http的retry。