

A silhouette of a person leading a camel across a desert dune at sunset. The sun is low on the horizon, creating a bright glow behind the figures. The sky is a clear, deep blue.

交易风险防控实务

风控部产品技术总监-刘光昕

主讲人背景

刘光昕

1. 2013年6月加入去哪儿网，负责支付中心风控团队
2. 曾负责易宝支付的风控体系建设，和来自支付宝风控的同事合作，从无到有打造新一代的风控系统并取得良好效果，针对大量的钓鱼案件提出创新式的策略进行了有效打击；
3. 曾在19pay任职，负责支付及电商团队的管理工作，用自己对于支付的理解，完成支付平台从无到有的设计开发及运营支撑，设计出灵活及安全的支付架构体系。在支付安全体系方面有独到的见解，曾轻易利用漏洞攻破易宝账户并告知对方

在线业务-钓鱼案例及对策

案例一：普通钓鱼-发送虚假支付链接

案例二：木马钓鱼-替换支付订单

案例三：普通钓鱼-发送虚假网址
盗号

普通钓鱼-发送虚假支付链接

案例介绍：

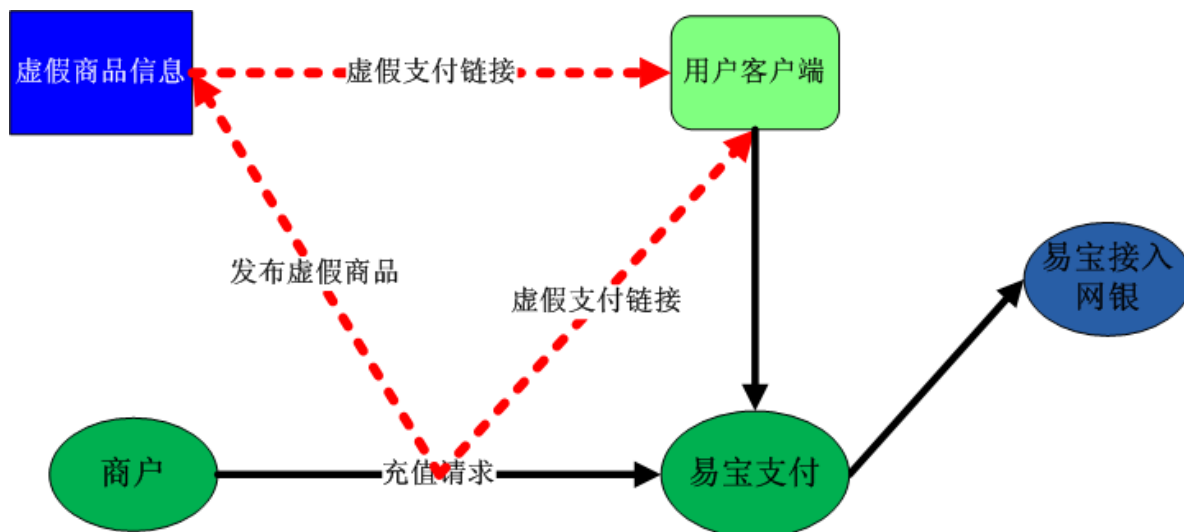
- 1 用户在淘宝购买价格低于市场的物品，通过旺旺接受卖家发的支付链接，跳到网银，用户用网银完成付款后，网银提示支付成功，但淘宝仍然是未支付状态,卖家也下线不再出现了
- 2 用户登录网银，查询到银行实际已经扣款，收款方为北京通融通信息技术有限公司
- 3 用户通过易宝客服获悉，支付的金额是为易宝会员账户充值，同时帐号中的钱已经购买电子点卡之类的虚拟货物

虚假支付链接示意图-商户到易宝

案例分析：黑客利用的是商户到易宝支付端协议的缺陷

特征: 1 黑客预先下好订单， 下单到支付的时间较长

2 发起方是在用户端， 所以易宝接收到的refer为空



应对措施

根据虚假支付链接利用商户到易宝支付协议缺陷的特征,采取了以下措施：

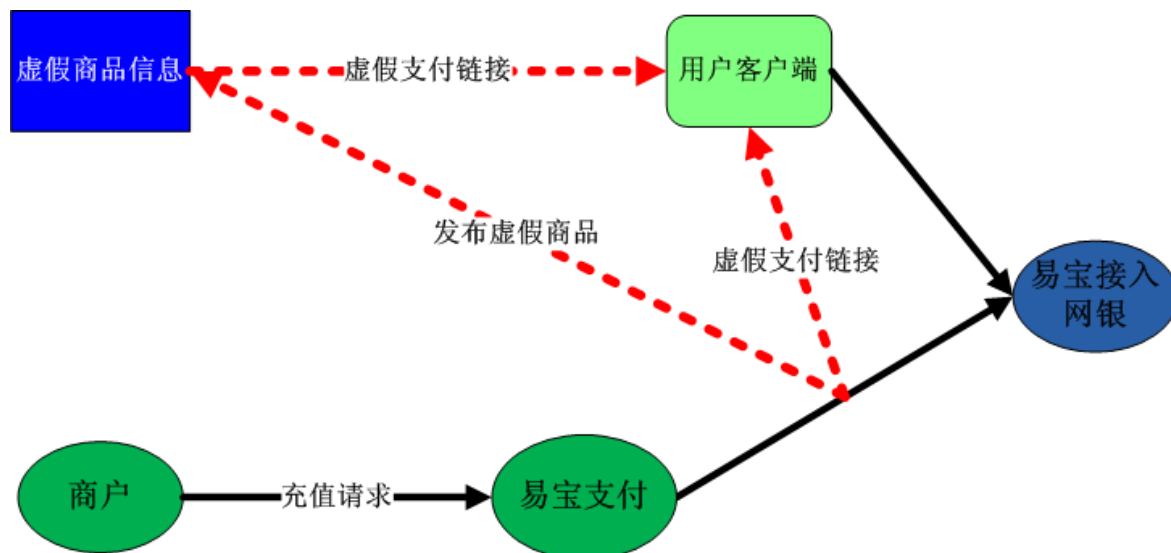
- 1 a 预先设置好商户网站的地址，在用户发起支付时读取reffer 中的地址和设置好的地址进行匹配
b 同时在接口协议中，增加用户在商户访问时的IP地址，发起支付易宝获取的访问IP和用户商户段的IP比较
如果a 和 b 都不符则拒绝支付
- 2 在支付接口协议中增加时间戳，在商户发起支付前将时间戳加入协议中，在用户发起支付时判断时间差，如果时间差大于1分钟则拒绝支付

虚假支付链接示意图-易宝到网银

案例：黑客利用的是易宝支付到网银端协议的缺陷

特征：1 发起方是在用户端，所以网银接收到的referrer为空

2 用户下单时，易宝获取到下单IP,网银支付成功后，页面跳回到易宝支付，易宝支付获取的支付IP 和下单IP不一致



应对措施

根据虚假支付链接利用易宝支付到网银协议缺陷的特征,采取了以下措施:

- 1 推动网银预先设置好商户网站的地址, 在用户发起支付时读取reffer中的地址和设置好的易宝支付地址进行匹配, 如果不符则拒绝支付
- 2 当用户在网银端支付完成, 跳回易宝页面时获取IP为支付IP, 对易宝下单的IP和支付IP进行比较, 如果不符则拒绝发货, (存在的问题, 页面异常导致依靠接受网银后台通知则失效)

措施比较: 第一项措施比较有效, 但存在网银差异推动难的问题

第二项措施为补充措施, 在前台通知能返回的情形下才有效

木马钓鱼-替换支付订单

案例介绍：

1 用户在淘宝购买东西，接受黑客发的文件并执行后，使用支付宝跳到网银，用户用网银完成付款后，网银提示支付成功，但淘宝仍然是未支付状态

2 用户登录网银，查询到银行实际已经扣款，收款方为北京通融通信息技术有限公司

3 用户通过易宝客服获悉，支付的金额是为易宝会员账户充值，同时帐号中的钱已经购买电子点卡之类的虚拟货物

案例分析

案例分析：

- 1 对于传统钓鱼，一般是由黑客下单，用户被骗支付，有明显的特征，就是下单的IP地址和支付的IP地址不一样，会被支付系统风控措施拦截，调取的数据显示，下单IP和支付IP完全一致
- 2 既然下单IP和支付IP，那只有一种解释，就是用户自己完成登录到易宝会员系统，发起充值跳到银行完成支付，这只有一种可能，那就是木马干的
- 3 木马可以完成篡改支付的跳转，但木马要完成登录到易宝账户的过程，几乎是不可能，因为易宝登录时增加了验证码，并且是复杂度极高汉字验证码

案例分析

4 分析木马的可能采取的方案：一是绕过验证码，那就是易宝存在不登录就能发起充值的入口，经过排查，没有这种可能，二是木马破解了易宝的验证码，那么木马是如何破解的呢

线索：

- 1 通过对受害客户的调查，找到木马的样本并且进行脱壳分析了，基本了解木马能躲避安全软件和IE安全的防范。
- 2 对木马的运行情况和报文数据进行分析，彻底了解了木马的工作原理和如何破解验证码
- 3 在淘宝发起交易观察木马替换链接的过程
接下来是木马替换过程的截图和说明：

木马钓鱼-替换支付订单

被钓鱼的支付宝界面一，注意：验证码实际为91.com 的登录验证码，91.com 已经在验证码上加了LOGO，但LOGO在验证码中不突出

支付宝  | 收银台

您好，刘光昕（支付宝账户：topliu@yahoo.com ）支付遇到问题？

1、确认购买信息 → 2、付款到支付宝 → 3、卖家发货，买家确认收货 → 4、支付宝付款给卖家 → 5、双方互相评价

订单名称	收款方	订单金额
正品贝尔金 Belkin... 详单	北京宝锐通创科技中心	61.00 元

付款方式： **中国工商银行** 储蓄卡 支付 **61.00** 元

请输入验证码： [看不清，换一张](#)

A630 

[登录到网上银行付款](#)

支付宝卡通：

免费升级到支付宝卡通，永久享受便捷付款
开通后无需登录网上银行，输入支付密码，即可完成付款。

[立即开通](#)

[选择其他方式付款](#) | [查看支付流程](#)

木马钓鱼-替换支付订单

升级后的验证码中

支付宝  | 收银台

您好, 刘光昕 (支付宝账户: topliu@yahoo.com ) 支付遇到问题?

1、确认购买信息 → 2、**付款到支付宝** → 3、卖家发货, 买家确认收货 → 4、支付宝付款给卖家 → 5、双方互相评价

订单名称	收款方	订单金额
正品贝尔金 Belkin... 详单	北京宝锐通创科技中心	61.00 元

付款方式:  **中国工商银行** 储蓄卡 支付 **61.00** 元

请输入验证码: [看不清, 换一张](#)

A630 

[登录到网上银行付款](#)

支付宝卡通:

免费升级到支付宝卡通, 永久享受便捷付款
开通后无需登录网上银行, 输入支付密码, 即可完成付款。

[立即开通](#)

[选择其他方式付款](#) | [查看支付流程](#)

木马钓鱼-替换支付订单

被钓鱼的支付宝界面二，注意：验证码实际为易宝会员的登录验证码，登录验证码为汉字,但没有加LOGO等水印



您好, 刘光昕 (支付宝账户: topliu@yahoo.com) 支付遇到问题?

1、确认合并付款信息 → 2、付款 → 3、付款完成

订单名称	订单金额
2笔购物 详单	406.60 元

付款方式:  招商银行 储蓄卡 支付 406.60 元

验证码: 阳些 看不清, 换一张

[登录到网上银行付款](#)

支付宝卡通:

免费升级到支付宝卡通, 永久享受便捷付款
开通后无需登录网银, 输入支付宝密码, 即可完成付款。

[立即开通](#)

[选择其他方式付款](#) | [查看支付流程](#)

木马钓鱼-替换支付订单

被钓鱼的网银界面，替换支付订单后，收款方为:快钱支付

ICBC (国) 中国工商银行 客户订单支付服务

帮助

【订单信息】

商城名称：快钱
订单号：110412217434
订单金额：RMB 61.00
商品名称：快钱支付
商品数量：1
收货地址：www.99bill.com

💡 请您仔细核对上述订单信息，确认无误后按照以下流程进行支付。

【银行支付】

① 请检查IE上的安全挂锁标识 

② 请输入支付卡(账)号和验证码

支付卡(账)号：

请输入右侧显示的验证码：



[刷新验证码](#)

③ 提交后请核对您的预留验证信息(点击查看说明)

提交

重填

如果您不是中国工商银行的网上银行注册用户，或需要设置预留信息，请到柜台办理有关手续。

+ 小e安全检测

工行支付服务提示

尊敬的客户，为保障您的支付安全，请在支付环节注意核对下列信息：

1. IE地址栏应以https开头
2. 本页面域名为mybank.icbc.com.cn或b2c.icbc.com.cn
3. IE浏览器应在右下角或正上方显示安全挂锁 
4. 本页面只需输入支付卡号和验证码，无须输入网银登录密码

如有疑问，请咨询95588。

木马钓鱼-替换支付订单

被钓鱼的网银界面，木马迅速更改页面，显示由块钱支付变为支付宝，商品名称也该为支付宝交易款，用户很难察觉


ICBC  中国工商银行 客户订单支付服务

【订单信息】

商城名称：	支付宝（中国）网络技术有限公司
订单号：	110412217434
订单金额：	RMB 61.00
商品名称：	支付宝交易款
商品数量：	1
收货地址：	

 请您仔细核对上述订单信息，确认无误后按照以下流程进行支付。

【银行支付】

① 请检查IE上的安全挂锁标识 

② 请输入支付卡(账)号和验证码


支付卡(账)号：

请输入右侧显示的验证码：

[刷新验证码](#)


③ 提交后请核对您的预留验证信息(点击查看说明)

如果您不是中国工商银行的网上银行注册用户，或需要设置预留信息，请到柜台办理有关手续。

 小e安全检测

工行支付服务提示

尊敬的客户，为保障您的支付安全，请在支付环节注意核对下列信息：

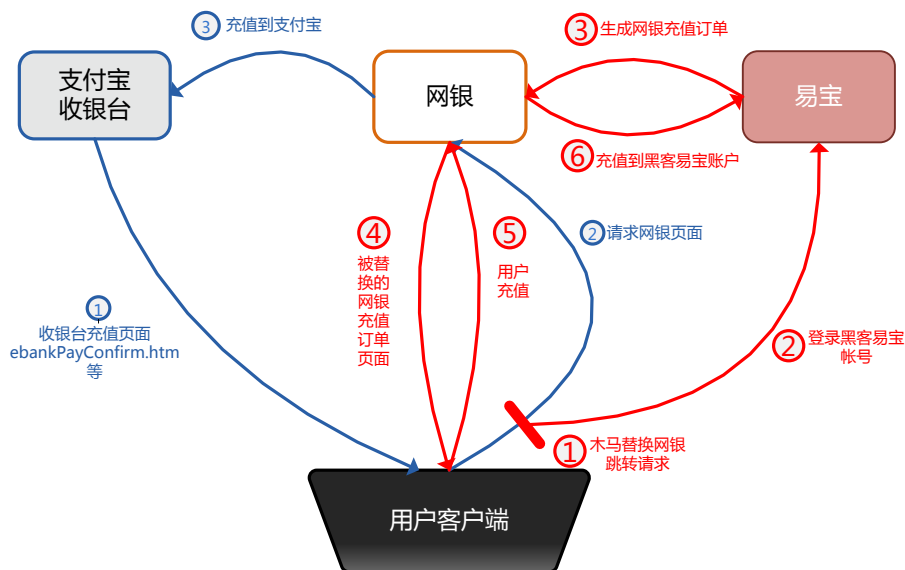
1. IE地址栏应以https开头
2. 本页面域名为mybank.icbc.com.cn或b2c.icbc.com.cn
3. IE浏览器应在右下角或正上方显示安全挂锁 
4. 本页面只需输入支付卡号和验证码，无须输入网银登录密码

如有疑问，请咨询95588。

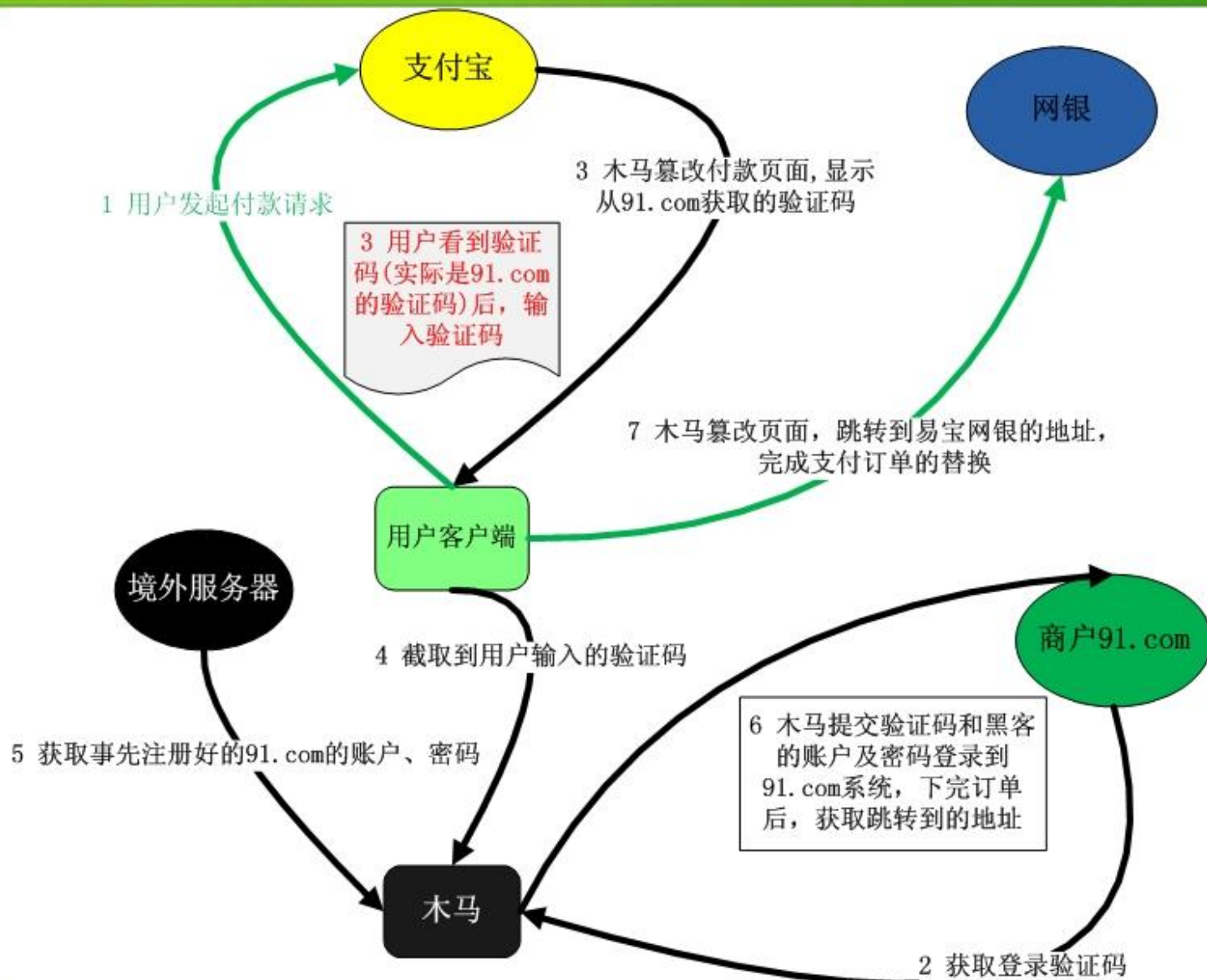
木马替换支付订单示意图

从页面中读取用户支付金额，并在用户支付或网银付款的页面，替换支付订单，付款到第三方支付平台。

(蓝色为正常交易流程，红色为被木马劫持后的流程)



木马替换支付订单具体手段

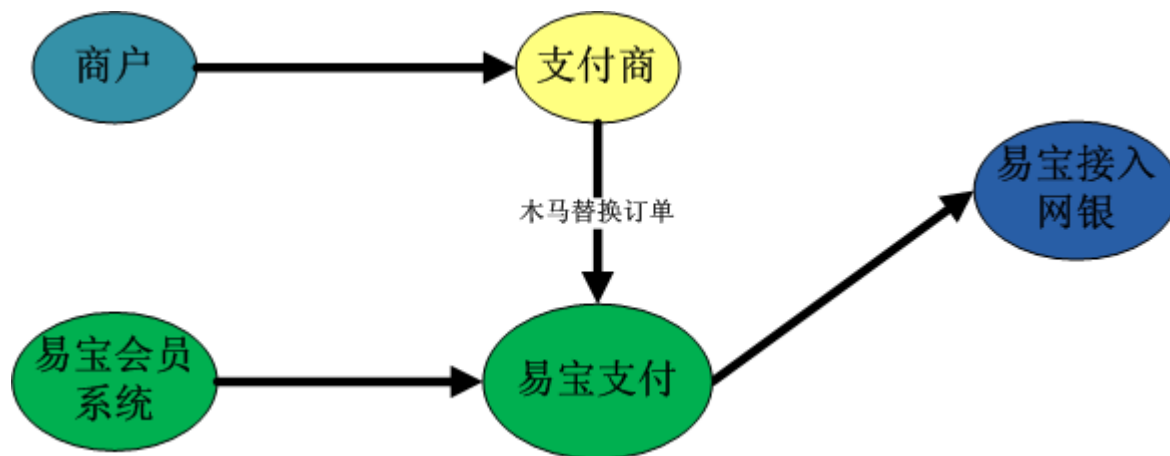


浏览器流程对比

正常浏览器流程:



被木马替换的浏览器流程:

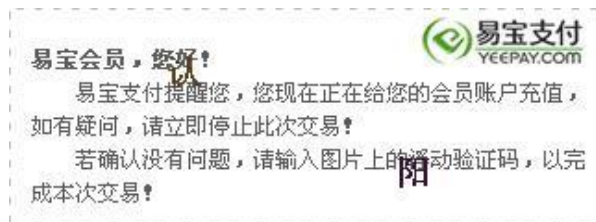


应对措施

根据木马破解验证码的方法,考虑采取以下措施:

- 1 易宝验证码不能被其它网页引用,但分析的结果显示,木马并不是在支付宝网页中直接引用,而是下载到本地后,在支付宝网页中引用本地的图片,所以该措施只起到补充防范的作用
- 2 改进验证码,带有明显易宝LOGO和提醒文字的背景,达到提醒用户的目的,这是目前比较有效的措施,验证码在图中出现的位置不固定,需要在商户系统中推广带提醒背景验证码。

如图所示:



同行验证码推广-快钱

快钱将新验证码方案
在网关上推广：
验证码：+变化的验证码



整体效果图：



快钱验证码被破-升级版本

验证码升级要点:

- 1 取消了验证码提示
- 2 验证码分散

N6 请确认以下支付信息: **5**

商家名称: **完美世界(北京)网络技术有限公司**

商品名称: 120

支付金额: 120元 **G**



整体效果图:

A diagram of the payment confirmation interface. It contains the same merchant and item information as the previous block, but with the "验证码" (verification code) field highlighted. Below the information is a dashed line, followed by the text "请输入上面浮动的4位字符验证码(从左至右):" (Please enter the 4-character floating verification code from left to right:), a text input box, and a "换一张" (Change one) link. At the bottom are two buttons: "确认支付" (Confirm Payment) with a red arrow icon and "取消" (Cancel).

快钱验证码二次被破-升级版本

验证码升级要点:

- 1 验证码字体颜色和背景一致
- 2 加入干扰线条

请确认以下支付信息:

商家名称: 完美世界(北京)网络技术有限公司

商品名称: 108

支付金额: 108元

支付系统提供商

快钱
99bill.com | 支付

整体效果图:

请确认以下支付信息:

商家名称: 完美世界(北京)网络技术有限公司


商品名称: 108

支付金额: 108元

支付系统提供商

快钱
99bill.com | 支付

请输入上面浮动的4位字符验证码(从左至右): 换一张

 确认支付

取消

快钱验证码-升级 FLASH 版本

整体效果图:

请确认以下支付信息:

商家名称: 完美世界(北京www)网络技术有限公司

商品名称: 3004 8 8 8 8

支付商: 快钱

支付金额: 3124元

请输入浮动的四位字母验证码: [换一张](#)

[取消](#)

如以上订单信息无法正常显示, 请点击安装Flash播放器
快钱版权所有

快钱验证码-FLASH破解

请确认以下支付信息:


商家名称: 完美世界(北京www)网络技术有限公司

商品名称: 300888

支付商: 快钱

支付金额: 3124元

请输入浮动的四位字母验证码: [换一张](#)



Method	Re...	URL
GET	304	http://localhost:8080/prepaycheck_091207.js
GET	304	http://localhost:8080/payCheck_0513.swf
GET	304	http://localhost:8080/navbar.js
GET	304	http://localhost:8080/gateway_110224.js
GET	200	http://localhost:8080/gateway/validatecode/getPayInfo.htm?signMsg=97fd4ab625a1314d5e3ead03c8fa0c4d&datetime=1411636724465
GET	304	http://localhost:8080/creditcheck_110315.js
GET	304	http://localhost:8080/
GET	404	http://img.99bill.com/seashell/gateway/validatecode/flash/js/swfobject_modified.js
GET	ERR...	http://:/

15 → 18 requests

快钱验证码-FLASH破解

```
import flash.display.*;
import flash.external.*;
import flash.net.*;
import flash.system.*;

public class _P1_ extends MovieClip {

    private static var hexChars:String = "0123456789abcdef";

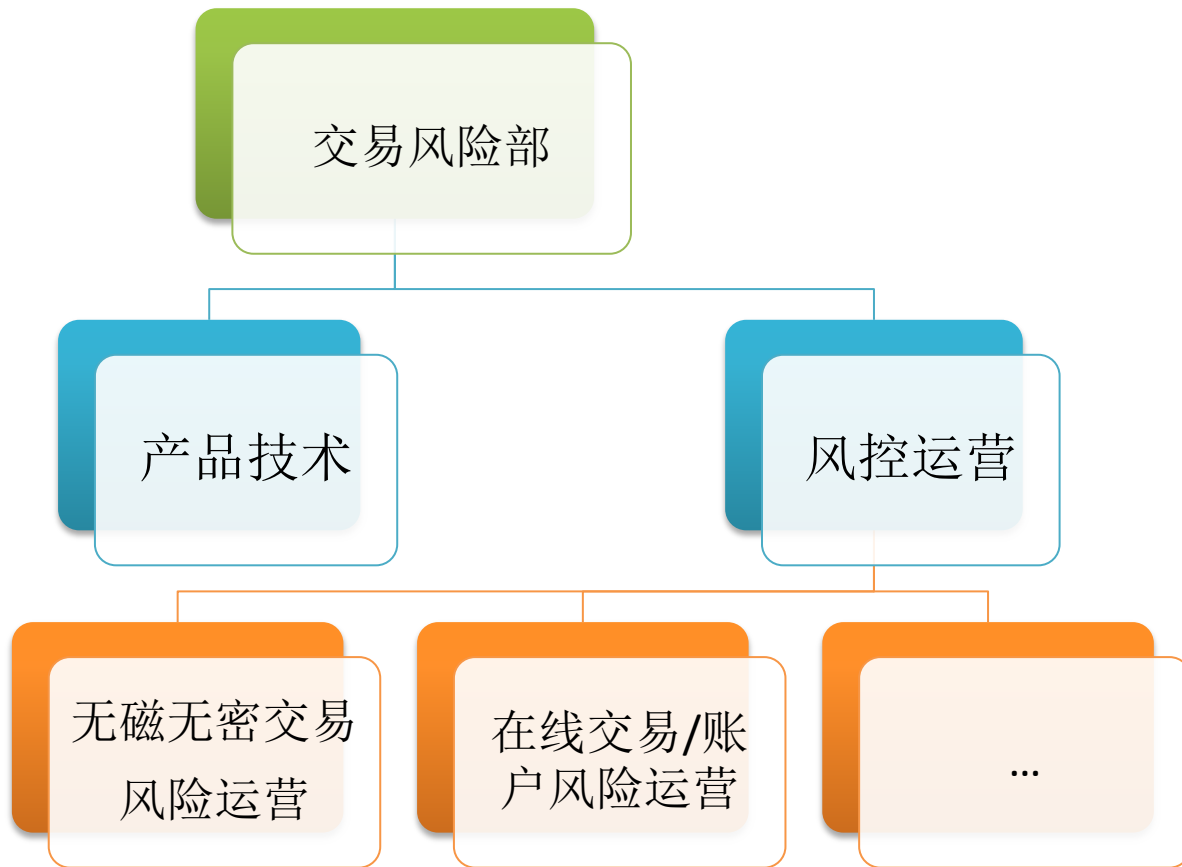
    public var validateCodeShow:TextField;
    private var _P6_:String = "/gateway/gatewayPhishing.htm";
    public var pay_btn:SimpleButton;
    private var sessionId = "";
    private var _P2_:URLLoader;
    private var _P11_:String = "http://club.99bill.com/viewthread.php?tid=128875";
    public var cancel_btn:SimpleButton;
    public var amount:TextField;
    public var productName:TextField;
    public var errorMsg:TextField;
    public var validateCode:TextField;
    public var refreshcode_btn:SimpleButton;
    private var _P8_:String = "/gateway/validatecode/getPayInfo.htm";
    private var _P14_:String = "NOTFRAUD";
    public var membername:TextField;

    public function _P1_():void{
        _P2_ = new URLLoader();
        super();
        System.useCodePage = true;
        var _local1:Object = stage.loaderInfo.parameters;
        if (_local1.sessionId != null){
            sessionId = _local1.sessionId;
        };
        if (_local1.errorMsg != null){
            errorMsg.text = _local1.errorMsg;
            return;
        };
        var _local2:Object = root.loaderInfo.parameters;
```

概述

- 在线业务-钓鱼案例及对策
- 风控管理架构
- 风控体系
- 风险分类及防控措施

管理架构



管理架构-产品技术



组长

- 组建并管理风控技术团队，领导产品及研发团队完成指定目标
- 根据公司风险管理战略及业务发展目标，搭建公司的风险管理体系；

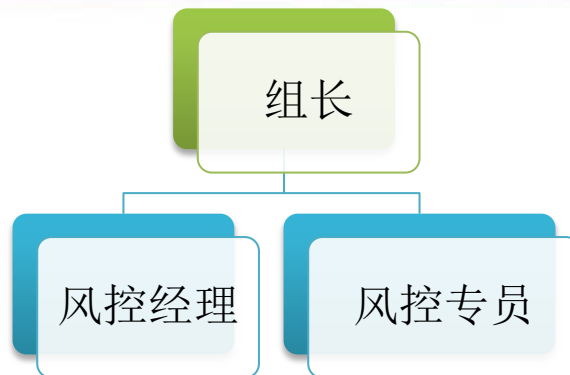
产品经理

- 参与新业务、产品的评审，识别、评估各项风险，提出风控建议并提供支持；
- 收集风控运营需求，形成产品文档并协调开发人员、测试人员完成开发上线

研发工程师

- 根据组长的开发安排开发风控基础系统并进行优化
- 根据产品经理的产品文档，形成概要设计、开发方案进行开发、测试及上线

管理架构-风控运营



组长

- 负责对风控运营小组的组建及管理工作
- 根据实际运用情况和产品技术小组提出风控需求

风控经理

- 制定风险处理流程, 定期出风险报告, 安排组员对RMCS的风险事件分工处理
- 建立和银行、商户之间的接口联系

风控专员

- 根据组长的安排对业务的RMCS的风险事件进行核查及处理
- 对风险案件进行处理, 联系银行、商户对风险案件的协调处理

风控体系

外围风控产品

- 安全控件
- 机器识别
- 数字证书
- 手机动态口令
- 防钓鱼网关
- 防木马钓鱼网关

RMCS风险拦截

- 风控防火墙规则实时拦截
- 大额交易控制
- 黑名单拦截

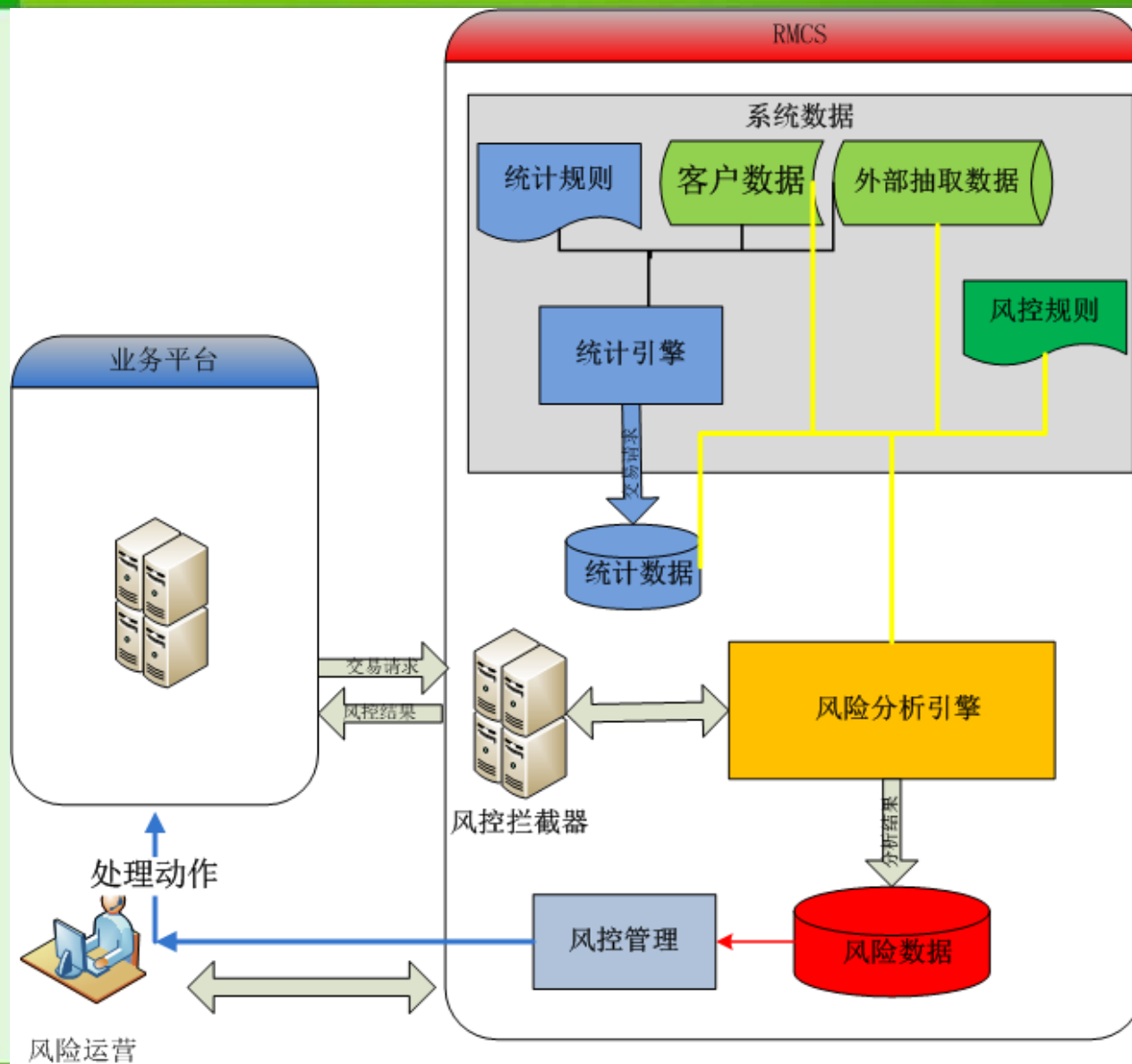
RMCS实时风险分析

- 数据抽取/采集
- 实时统计集群
- 规则维护
- 实时分析引擎
- 阻断黑名单
- 可疑黑名单
- 可信白名单
- 实时预警

人工核查

- 案件受理及跟踪
- 风险事件处理
- 大额交易核查
- 账户冻结处理
- 商户信息变动审核
- 案件库管理

风控体系-运行示意图



统计引擎：根据统计规则进行统计，可以设置交易数据的任何字段进行统计，输出的结果是统计数据



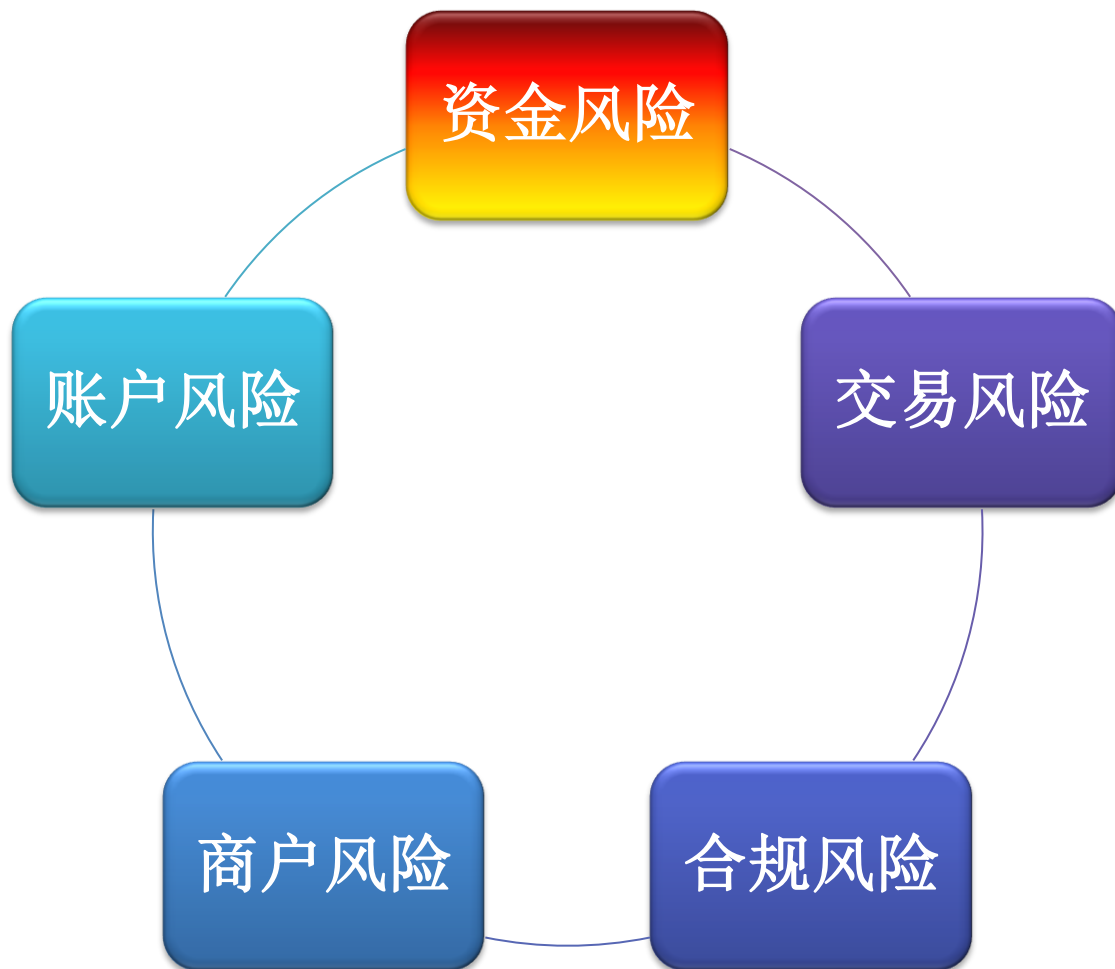
分析引擎：根据风险规则进行判定，可以调用统计规则，引用统计数据，输出的结果是风险数据



处理动作：在判定为风险事件后，根据风险规则设置的行动通知业务平台进行相应的处理

风险分类及危害

风险分类根据不同维度有不同的定义，以下为在实际运营中对风险进行归纳做出的分类



风险分类及危害

资金风险

- **资金风险**是指用户利用资金链环节的缺陷获利，造成资金亏损，损失资金无限放大

交易风险

- **交易风险**是指黑客利用交易环节中的缺陷获利，导致实际付款用户受损，支付商也可能承担责任

账户风险

- **账户风险**是指黑客利用非法手段操控账户，获取账户中的资金，导致账户拥有者带来资金损失

商户风险

- **商户风险**是指由于商户运营非法给用户造成损失，支付商也可能承担责任

合规风险

- **合规风险**是支付商由于违反法律、央行规定运作而面临处罚的风险



后果

品牌受损

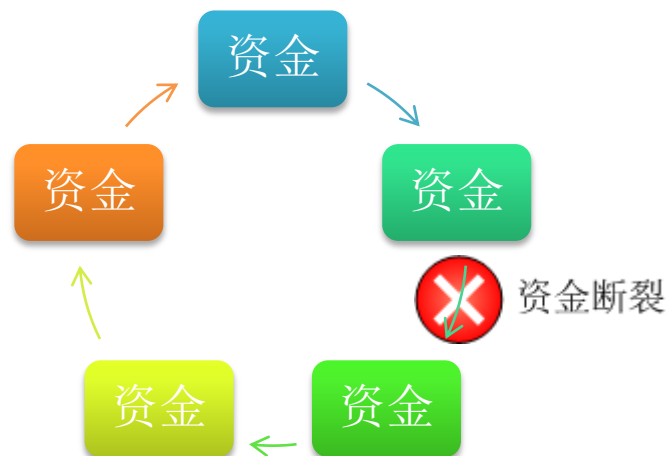


资金损失



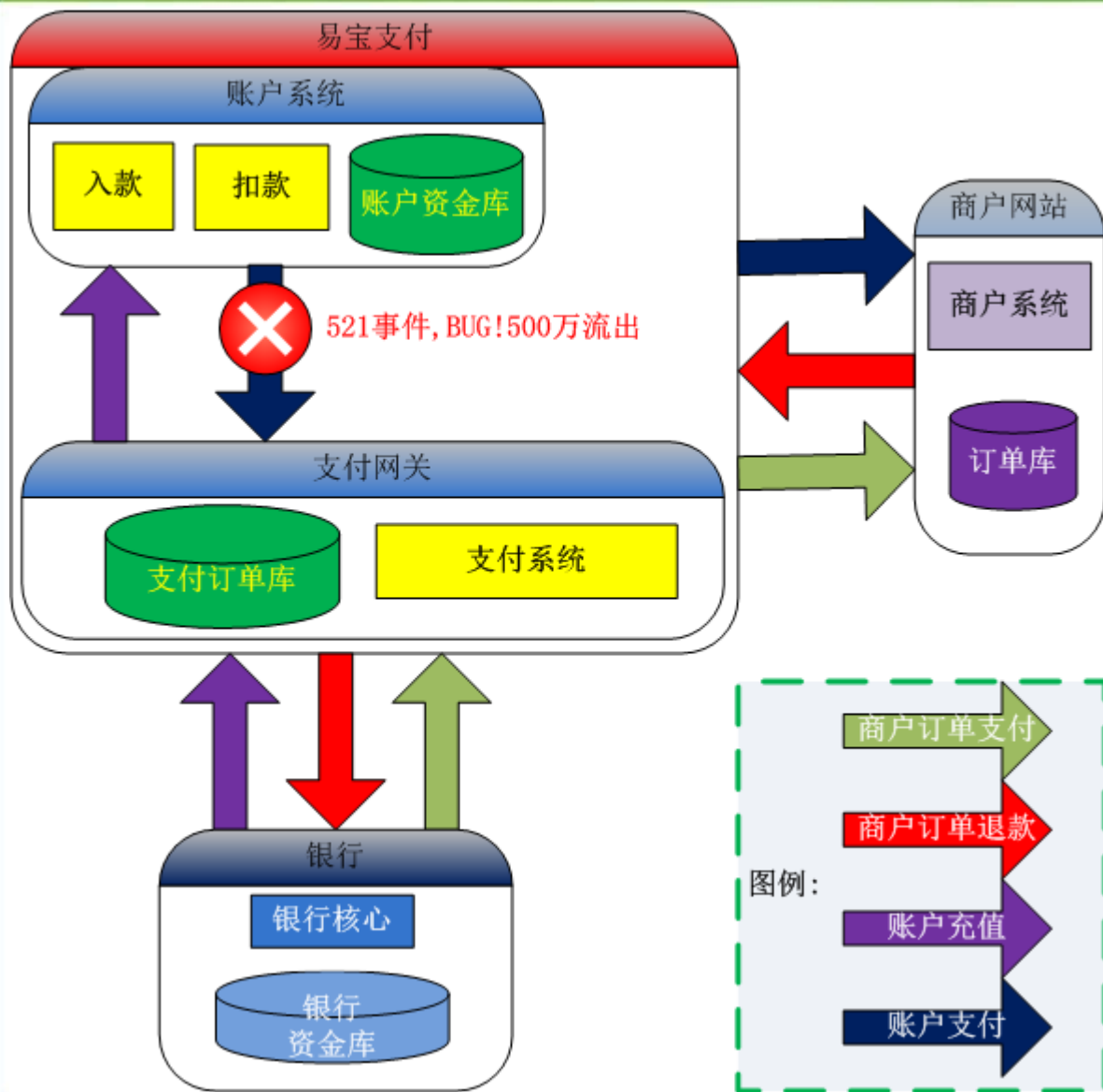
运营资格

资金风险是指用户利用资金链环节的缺陷获利，导致资金流入流出不平衡，造成资金亏损



如：易宝支付521事件,由于系统BUG,造成账户支付没有扣款,支付网关订单却支付成功, 损失金额 500 多万

资金风险-资金流示意图



要做好资金风险
防控，必须先了解
资金流向

账户系统充当
2个角色

充值时： 商户
账户消费： 银行

图例：

商户订单支付

商户订单退款

账户充值

账户支付

资金风险-防控措施

防控措施：检查资金链流出和流入是否匹配，
将以下措施通过RMCS 配置规则实现风险预警

账户支付

- 关联账户扣款记录和支付订单(支付通道为账户)记录
- 检查是否存在扣款记录, 比较金额

账户充值

- 关联账户入款记录和支付订单(商户为账户)记录
- 检查是否存在支付订单记录并比较金额

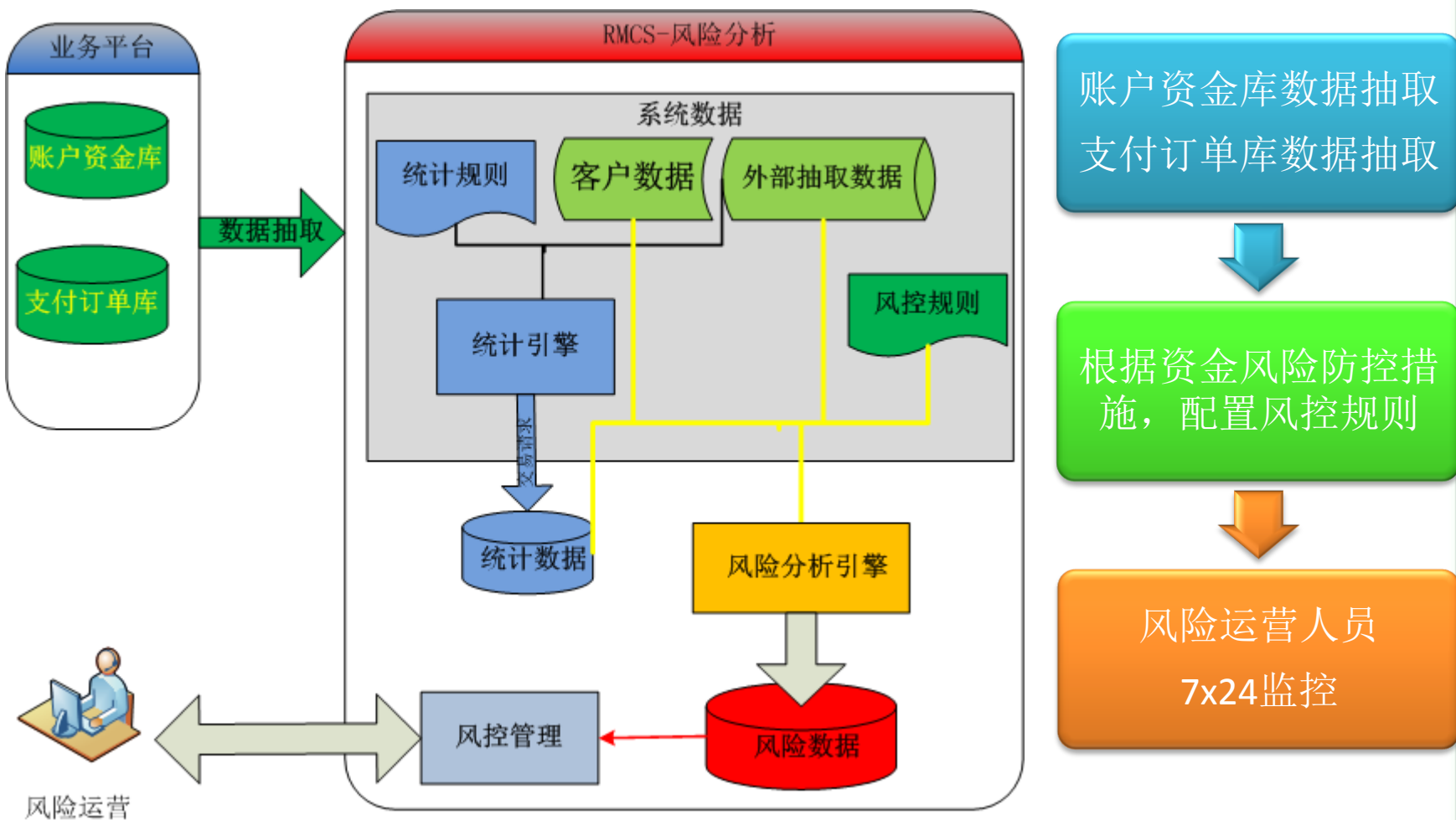
商户消费

- 通过银行接口发起支付状态查询并记录
- 检查支付订单记录和支付状态查询记录金额是否一致

商户退款

- 检查相同订单累计退款金额是否小于订单支付金额
- 检查同一个商户的退款比例

资金风险-防控措施



交易风险

交易风险是指黑客利用交易环节中的缺陷获利,导致实际付款用户受损



木马钓鱼

- URL链接钓鱼
- 木马钓鱼

银行卡被盗

- 钓鱼网站
- 用户密码泄漏

交易风险-主要防控措施

大额交易控制措施



高频度交易控制措施



交易链路检查措施

交易风险-大额交易

大额交易被钓鱼给单个用户带来巨大的损失，虽然法律判定用户是责任方，但仍然会导致用户采取一切激烈的措施来挽回损失，比如：上诉，集体到支付公司维权等



交易风险-高频度交易

在银行卡被盗或系统存在漏洞时，由于交易单笔金额的限制，获利者采取多次交易的方式实现最大利益



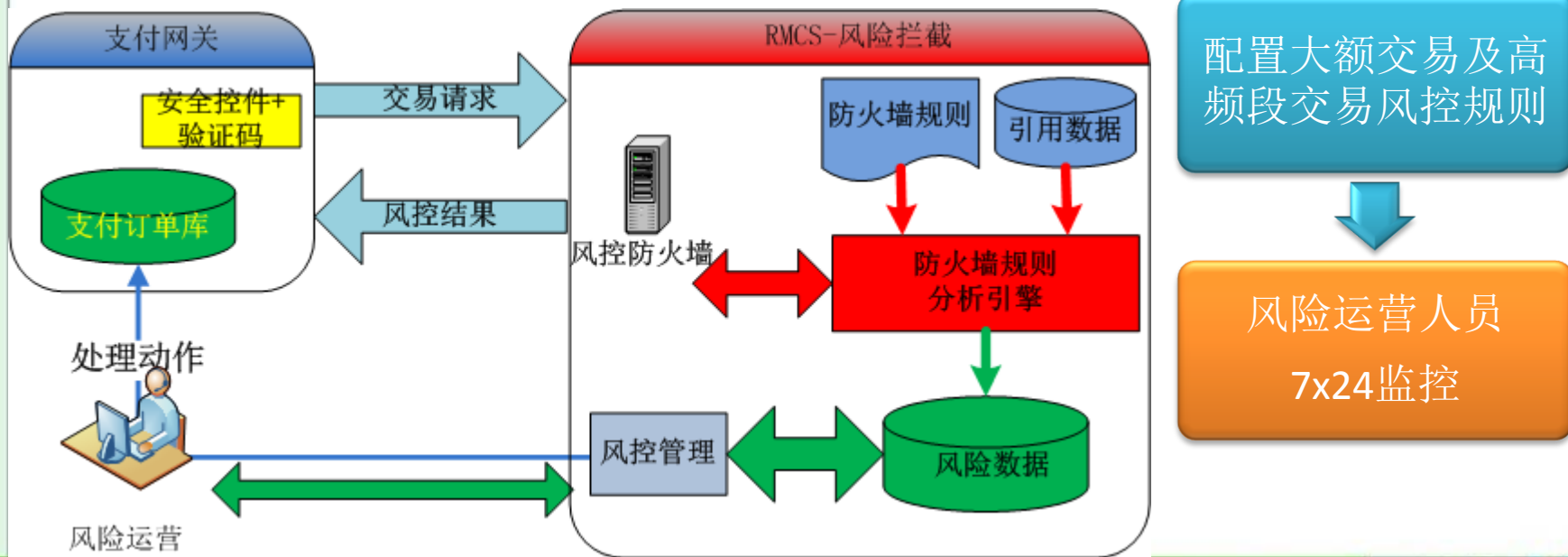
交易风险-大额及高频度交易控制

大额交易控制

- 安全控件+验证码，木马防控有效手段
- 收集客户信息，判断客户是否可信
- 首笔人工核查，滞留时间为用户提供反馈机会

高频度交易控制

- 计算客户识别的交易频次及累计金额
- 根据风控规则进行限制
- 人工核查



交易风险-客户识别的重要性

风险拦截

规则

客户识别

你是谁

客户识别

- 一个客户可以发生多次交易行为，客户识别的准确性在风控体系中非常重要

方法

- IP地址，MAC地址，银行卡号，客户端软指纹，Cookie/flash Cookie串，手机号，身份证号等

识别用途

- 通过相同的客户识别方式，关联出同一个客户的所有行为，利用规则判断该客户操作行为是否风险

拦截用途

- 在识别出该客户行为风险行为后，就可以拦截该客户的任何操作行为

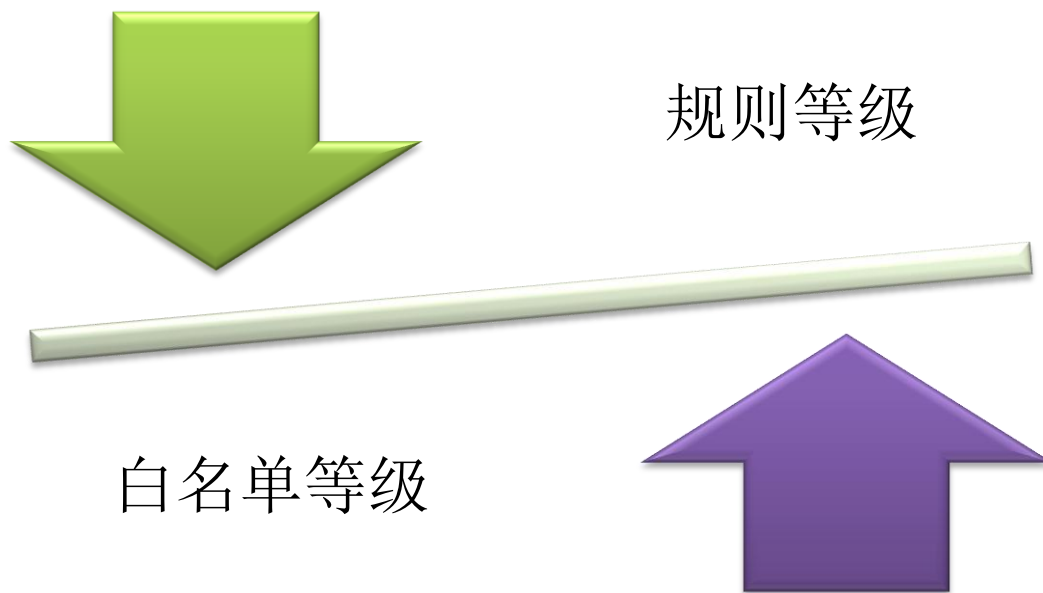
交易风险-客户白名单

白名单是指客户曾经发生过交易，事后无风险

作用范围：业务系统、事件、规则

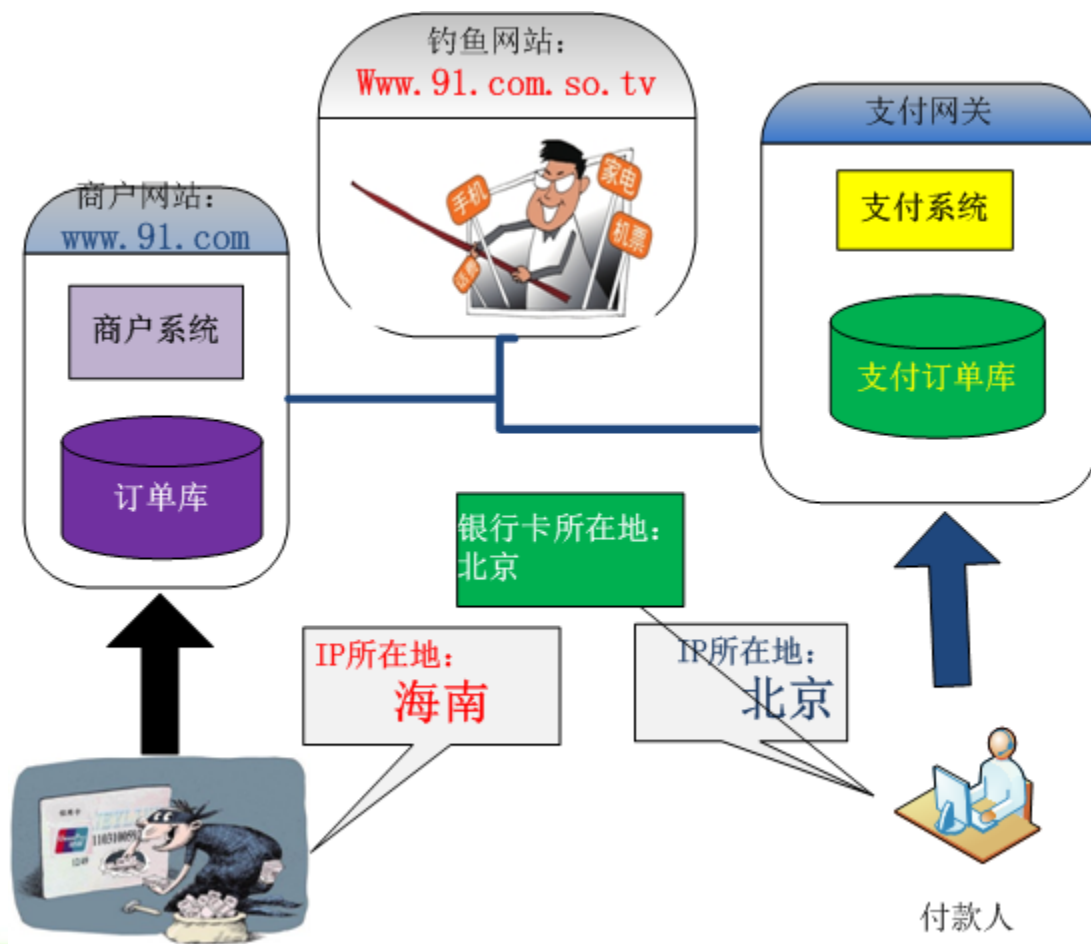
风险等级：对客户进行分析后得出风险等级，该等级和规则中的风险等级形成梯次免疫模型

多维组合：多个客户属性形成一个白名单，比如：卡号+手机号



交易风险-交易链路检查措施

通过IP、银行卡号识别付款人，REFER判断订单来源对交易链路进行检查



交易风险-交易链路检查措施

IP/卡号识别

- IP库,银行卡号库获取所在地
- 下单和支付IP所在地比较
- 银行卡号所在地和客户端所在地(IP所在地)

时间戳

- 设置订单有效时间
- 支付时和下单时间比较

订单来源识别

- 读取订单来源识别Reffer参数
- 将订单来源识别Reffer与预先设置比较

增强验证码

- 将订单信息和验证码整合为不可分割的验证码产品
- 增加密码控件对输入的验证码进行加密,后端进行解密

账户风险

账户风险是指黑客利用非法手段操控账户，获取账户中的资金，导致账户拥有者带来资金损失



安全认证产品

二次验证

数字证书

支付盾

第三方盾

手机动态口令

宝令

手机宝令

账户风险

马奇诺防线:账户安全产品众多，每个产品很安全，黑客采取迂回战术,通过一个点瓦解所有防线

误区：有安全产品，
安全没问题

安全认证产品

二次验证

数字证书

支付盾

第三方盾

手机动态口令

宝令

手机宝令

短信操控

找回密码

取得账户操控

支付宝账户被盗系列:

1. 手机卡无端被补办 支付宝账户被盗
2. 支付宝用户短信被转移 银行账户被盗千元

账户风险

账户的被盗分为直接和间接的手段，直接指黑客直接获取帐号密码，间接指黑客破解依赖的短信、邮箱再找回密码



直接

木马盗号

钓鱼网站

间接

短信窃取

邮件窃取

账户风险-防控措施

防控重点：解决单因子依赖，用双因子验证

登录检测

- 客户端信息异常,ip异地登录, mac 异地登录
- 相同客户端登录次数、账户数异常
- 大资金客户可疑登录及时冻结, 人工核查

找回密码检测

- 当天有登录记录或交易记录不允许找回
- 可疑客户端密码找回需要人工核查

注册检测

- 同客户端注册数量超限
- 客户端所在地与注册地址不匹配
- 可疑注册需要人工核查

账户其他

- 短信解绑证书
- 帐户变更
- 高频度交易控制
- 大额交易控制

商户风险

商户风险是指由于商户运营非法给用户造成损失，而支付提供者可能要承担连带责任

典型的有：

1. 商户欺诈，比如收款不发货，结算后退款
2. 商户运营不合规，比如出售违禁品

事前
商户准入

- 身份及银行卡信息认证
- 网站浏览，内部黑名单数据过滤
- 营业执照、经营范围审核

事中商户审查

- 商户网站定期合规检查，人工核查，商户上门拜访
- RMCS 违禁品关键字的搜索引擎检查，RMCS自动分析
- 交易量异常波动商户核查,高危商户定期审查
- 商户退款频次监控, 风险预存期控制，

合规风险及防控措施

合规风险是由于违反法律、央行规定运作而面临处罚的风险

典型风险：反洗钱

内部控制措施

- 完善的内部控制制度管理体系

客户身份识别

- 多方式、多手段核实客户身份
- 高风险客户开展强化尽职调查

可疑交易监控

- 应用符合行业特点的反洗钱监测管理平台
- 对可疑交易进行监控、分析、上报

资料保存

- 客户身份资料和交易资料长期保管
- 做到可追溯、可还原交易

结束语

谢谢!