ICS 35.240.15
L63

T/PCAC

中 国 支 付 清 算 协 会 标 准

T/PCAC 0006—2019

条码支付移动客户端软件检测规范

Testing specification on mobile client software for bar code payment

2019 - 02 - 01 发布　　2019 - 02 - 01 实施

中国支付清算协会安全与技术标准专业委员会 发布

目　　录

前　言

本指引由中国支付清算协会提出。

本指引由中国支付清算协会技术标准工作委员会归口。

本指引主要起草单位：中国支付清算协会、中国工商银行、中国银行、中国建设银行、中国银联股份有限公司、网联清算有限公司、北京中金国盛认证有限公司、中国网络安全审查技术与认证中心、北京银联金卡科技有限公司、中金金融认证中心有限公司、支付宝（中国）网络技术有限公司、财付通支付科技有限公司、福建联迪商用设备有限公司、福建新大陆电脑股份有限公司等单位。

本指引主要起草人：蔡洪波、马国光、邢桂伟、于沛、欧阳明、侯晓晨、侯玉华、潘葛桐、秦湘清、蔡予萌、庄俊国、王媛媛、张萌、侯戬、魏一豪、曹宇、汪毅、严伟锋、薛文哲、陈贵阳、聂丽琴、付小康、陈兰朋、张健、毕强、孟飞宇、邢增辉、尚可、蒋利兵、李远、王鑫、李欧、张行、王飞宇、吴宝民、刘文其、吴军、曹小龙、姜志辉、吴永强、马松松、于海涛、彭波涛、叶芳耀、刘峰、卢佩新、吴万通、钟文斌。

本指引为首次发布。

条码支付客户端软件检测规范

1 范围

本规范规定了支持条码支付的移动客户端应用软件的检测要求。对于仅支持内容浏览等关联业务、不直接集成支付功能的应用软件的安全、移动支付终端操作系统安全、SE的安全均不属于本部分的规定范围。

本规范适用于移动终端应用软件检测机构以及设计、开发、集成、维护和运营单位。

依据本规范开展检测的条码支付移动客户端软件同时应符合《JR/T 0098.3 中国金融移动支付检测规范 第3部分：客户端软件》的要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 18030-2005 信息技术 中文编码字符集

GB/T 12905-2000 条码术语

GB/T 23704—2009 信息技术 自动识别技术与数据采集技术 二维条码符号印制质量的检验

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

JR/T 0098.3 中国金融移动支付检测规范 第3 部分：客户端软件

中国人民银行.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）.2016年6月15日

中国人民银行.中国人民银行办公厅关于印发《网络支付报文结构及要素技术规范（V1.0）》的通知（银办发〔2016〕222号）.2016年10月27日

中国人民银行.中国人民银行关于强化银行卡受理终端安全管理的通知.(银发〔2017〕21号).2017年1月22日

中国人民银行.中国人民银行办公厅关于加强条码支付安全管理的通知（银办发〔2017〕242号）.2017年12月22日

中国人民银行. 中国人民银行关于印发《条码支付业务规范（试行）》的通知.（银办发〔2017〕296号）.2017年12月25日

3 移动终端安全

3.1 人机交互安全

3.1.1 身份验证信息管理

3.1.1.1 原始身份验证信息保存

检测目的：检查原始身份验证信息是否保存在移动终端本地，如果是，是否以密文形式保存在移动终端本地并且在验证操作结束后是否及时清除明文缓存。

检测方法：如果原始身份验证信息保存在本地，检查保存在移动终端本地的身份验证信息数据，在验证操作结束后再次检查本地身份验证信息数据本地缓存数据。

通过标准：原始身份验证信息明文未保存在移动终端本地，并且在验证操作结束后及时清除了缓存。

3.1.1.2 交易密码限制与保护

检测目的：检查客户输入交易密码的复杂度、与个人信息的关联性。

检查输入交易密码是否提供即时加密功能。

检测方法：检查初始交易密码的使用和输入密码校验规则。

检查在输入交易密码过程中即时产生的交易密码数据。

通过标准：客户端软件限制了使用初始交易密码，对交易密码复杂度进行了校验，不采用简单交易密码、与客户个人信息相似度过高的交易密码，在客户输入交易密码过程中无明文交易密码数据残留。

3.1.1.3 密码设置引导

检测目的：检查是否存在提醒客户避免设置与常用软件、网站相同或相似的用户名和密码组合的提示信息。

检查是否采取了对客户设置独立的支付密码的引导措施。

检测方法：检查密码设置的流程和提示信息。

通过标准：存在提醒客户避免设置与常用软件、网站相同或相似的用户名和密码组合的提示信息，采取了对客户设置独立的支付密码的引导措施。

3.1.2 交易异常处理

检测目的：当交易出现异常时，检查客户端是否向客户提示出错等信息。

检测方法：模拟异常情况检查客户端的提示信息。

通过标准：当交易出现异常时，客户端向客户提示出错等信息。

3.2 客户端软件安全

3.2.1 数据有效性校验

检测目的：检查客户端软件是否对通过人机接口或通信接口输入的数据进行了有效性校验。

检测方法：检查客户端软件对输入数据的校验逻辑。

通过标准：客户端软件提供了数据有效性校验功能，保证通过人机接口或通信接口输入的数据格式或长度等信息符合系统设定要求，如输入的交易金额等信息不含特殊字符、负数等非法参数。

3.2.2 页面回退清除敏感信息机制

检测目的：当页面回退时，检查客户端软件是否支持清除密钥、密码等敏感信息的机制。

检测方法：检查页面回退后客户端软件中的敏感信息数据。

通过标准：客户端软件支持页面回退清除密钥、密码等敏感信息的机制。

3.2.3 反编译

检测目的：检查客户端软件是否采用了防逆向工程保护措施。

检测方法：对客户端软件进行逆向工程攻击。

通过标准：客户端软件采用了防逆向工程保护措施，如客户端软件采取代码花指令、反调试、代码混淆等技术手段，防范攻击者对客户端软件的反编译分析。

3.2.4 客户端软件完整性

检测目的：检查客户端软件的完整性，是否对客户端软件进行签名，是否标识客户端软件的来源和发布者，在客户端软件启动和更新时，是否进行真实性和完整性校验。

检测方法：检查客户端软件的签名，查看软件信息，在客户端软件启动和更新时，检查对客户端软件真实性和完整性校验逻辑。

通过标准：客户端软件进行了签名，标识了客户端软件的来源和发布者，在客户端软件启动和更新时，进行了真实性和完整性校验。

3.2.5 运行时安全

检测目的：检查客户端软件是否采取了木马病毒防范措施，检查是否进行了信息加密保护，检查是否对运行环境可信进行了监测，并向后台反馈移动终端支付环境安全状况。

检测方法：对客户端进行木马病毒攻击，检查其采取的防范措施以及向后台的反馈情况，尝试读取客户端存储信息。

通过标准：客户端软件采取了木马病毒防范措施，进行了信息加密保护，对运行环境可信进行了监测并向后台反馈移动终端支付环境安全状况，如系统管理员权限是否开启等。

3.3 通信安全

3.3.1 网络通讯协议

检测目的：检查客户端软件与服务器之间是否建立了安全的信息传输通道，通过公开网络进行数据传输时是否进行了双向认证，如果使用SSL/TLS协议，是否使用安全的版本。

检测方法：检查客户端软件与服务器之间通讯安全措施。

通过标准：在客户端与服务器之间建立了安全的信息传输通道。

如果使用SSL/TLS协议，宜使用如TLS1.2等更安全的SSL协议。

通过公开网络进行数据传输时，可通过密钥、证书等密码技术手段实现服务器与客户端之间的安全认证。

3.3.2 抗抵赖

检测目的：检查客户端是否对发送报文的关键要素进行数字签名，保证支付内容的真实性和抗抵赖性。

检测方法：检查客户端对发送报文的关键要素是否采用数字签名或报文鉴别码等方式。

通过标准：客户端对发送报文的关键要素采用数字签名或报文鉴别码等方式，以确保支付内容的真实性和完整性。

4 交易安全

4.1 基本要求

4.1.1 信息脱敏

检测目的：若客户端软件涉及银行卡卡号、卡片验证码、支付账户等信息，应进行脱敏处理，支持基于支付标记化技术的交易处理。

检测方法：检查支付标记化在条码支付中的资料说明，识读条码信息，测试其是否含有支付账号、银行卡信息等支付敏感信息。

通过标准：对银行卡卡号、卡片验证码、支付账户等信息进行了脱敏处理，支持基于支付标记化技术的交易处理。

4.1.2 密码算法

检测目的：检查客户端软件所使用的密码算法是否满足国家密码管理机构要求。
检测方法：检查客户端软件所使用的密码算法，并执行实际测试，验证密码算法运行的正确性。
通过标准：客户端软件所使用的密码算法使用了经国家密码管理机构认可的密码算法。

4.1.3 安全审计

检测目的：检查是否定期对支付敏感信息安全进行内部审计。
检测方法：检查客户端软件的资料说明和内部审计文档，检查支付敏感信息安全的审计流程。
通过标准：定期开展了支付敏感信息安全的内部审计。

4.2 码制

检测目的：检查一维码是否使用具有国家标准的码制，至少支持：
GB/T 12908-2002 《三九条码》
或 GB/T 18347-2001 《128 条码》
二维条码是否使用具有国家标准的码制，至少支持：
GB/T 18284-2000 《快速响应矩阵码》
检测方法：对条码编码、码制相关的文档进行检查。
通过标准：条码使用了具有国家标准的码制。

4.3 数据录入

4.3.1 敏感信息显示

检测目的：检查用户输入交易密码等敏感信息时，客户端界面是否是明文显示。
检测方法：查看资料说明中有关敏感信息显示的说明。
查看用户通过客户端软件登录时输入的登录密码是否默认以明文方式显示。
查看用户通过客户端软件进行支付操作时，输入的支付密码是否以明文方式显示。
若客户端软件中存在其他需要用户输入的敏感信息，则查看是否以明文显示。
通过标准：厂商声明与验证结果一致。
客户端默认不以明文显示登录密码。
客户端不以明文显示交易密码等敏感信息。

4.3.2 数据防窃取

参见 JR/T 0098.3 中的 6.5.1.1。

4.3.3 数据防篡改

参见JR/T 0098.3中的6.5.1.2。

4.4 数据访问

检测目的：检查是否能越过授权访问客户端数据。
检查客户端是否访问了移动终端中非业务必需的文件和数据。
检查支付敏感信息是否按照业务需求进行保存和使用，显示时是否进行屏蔽处理。

检测方法：查看资料说明的相关说明，检查客户端在操作系统提供的安全机制之外，采取哪些额外措施保护自身数据不被非法访问。

执行相关测试，如检查接口暴露级别、文件权限等，验证声明的访问控制措施是否正确实现。

检查支付敏感信息的保存和使用方式，是否遵从业务需求；检查支付敏感信息的显示，是否存在屏蔽处理。

通过标准：客户端根据业务需要保证支付敏感信息仅供授权用户或授权应用组件访问。支付敏感信息按业务需求进行保存和使用，显示时进行屏蔽处理。

4.5 数据存储

4.5.1 敏感数据存储

检测目的：检查在满足法律、管理规定的前提下，客户端是否保留最少的客户信息，并限制数据存储量和保留时间。

检测方法：检查有关客户端涉及条码数据的说明，检查客户端是否会将条码安全保存在文件系统中。

使用工具查看客户端保存的敏感数据是否与声明一致。

通过标准：客户端仅存储业务必需数据，敏感数据保存时进行加密或不可逆变换，敏感账户信息不存储。客户端将条码安全地保存在文件系统中。

4.5.2 残余信息保护

检测目的：检查敏感数据在使用完毕后，是否立即进行清除。

检查客户端软件退出时，是否清除非业务功能运行所必需留存的业务数据。

检查客户端软件卸载完成后，文件系统中是否残留与用户相关的个人信息及敏感数据等。

检测方法：查看资料说明或代码片段，检查敏感数据清除机制。

客户端软件退出时，检查是否清除了非业务功能运行所必需留存的业务数据。

卸载客户端软件时，检查文件系统是否残留用户相关的个人信息及敏感数据。

通过标准：敏感数据在使用完毕后立即清除，退出时清除非业务功能运行所必需留存的业务数据，卸载时一并清除与用户相关的个人信息及敏感数据。

4.6 数据传输

4.6.1 数据保密性

检测目的：检查敏感数据(如账户信息等)和条码信息在本地程序组件间或通过公共网络传输时，是否采取措施（如加密等）确保其保密性。

检测方法：查看资料说明，检查客户端会传输哪些敏感数据和条码信息，数据传输过程中是否进行了加密。

检查数据的加密算法、密钥长度及密钥管理方式是否符合国家密码主管部门以及金融行业相关技术标准的要求。

尝试截获传输报文，验证敏感数据和条码信息是否采取加密措施。

通过标准：传输过程中对敏感数据和条码信息进行了加密保护。

4.6.2 数据完整性

检测目的：检查关键的交易数据在本地程序组件间或通过公共网络传输时，是否采取措施（如MAC等）确保其完整性。

检测方法：查看资料说明，检查客户端会传输哪些关键的交易数据，如条码信息、收款人信息、交易金额、订单号等，数据传输过程中是否添加了完整性校验值。
检查产生完整性校验值的算法是否为 HMAC、CBC-MAC 或其他安全措施，校验值计算接口是否可被其它程序非法调用。
尝试截获传输报文，验证关键交易数据是否采取文档所声明的完整性校验手段。
通过标准：传输过程中对关键交易数据进行了完整性保护。

4.7 条码生成

4.7.1 基本要求

检测目的：条码生成时，是否对支付账号、银行卡卡号等信息进行脱敏处理。
是否防止生成的条码携带病毒、木马等恶意代码。
是否设置条码使用有效期。
是否采用有效措施，确保条码信息的真实性、完整性、一致性和不可抵赖性。
检测方法：检查资料说明和代码关于条码生成的过程，包括对支付账号、银行卡卡号等信息的脱敏处理方式，防止生成的条码携带病毒、木马等恶意代码的方式，条码使用有效期的处理方式，以及保障条码信息的真实性、完整性、一致性和不可抵赖性的实现机制。
通过标准：条码生成时，使用支付标记化技术对支付账号、银行卡卡号等信息进行脱敏处理。
确保生成条码软硬件的安全性，防止生成的条码携带病毒、木马等恶意代码。
根据风控能力，严格设置条码使用有效期。
应采用有效措施，确保条码信息的真实性、完整性、一致性和不可抵赖性。

4.7.2 收款扫码

4.7.2.1 基本要求

检测目的：客户端展示条码前是否进行身份认证。
是否限制条码的使用次数和展示周期。
是否具备防止截屏等方式窃取展示条码的措施。
生成条码时是否采用加密方式。
检测方法：执行收款扫码，检查客户端展示条码前是否进行身份验证。
检查条码的使用次数和展示周期。
尝试通过截屏等方式窃取展示条码，验证是否具备有效的防止措施。
检查生成条码时是否采用了加密的方式。
通过标准：采用收款扫码方式时，展示条码的客户端先进行身份验证。
条码限制一次使用且展示周期原则上不超过 1 分钟。
采取有效措施防止条码被截屏或截屏后条码无法使用。
采用加密方式生成条码。

4.7.2.2 服务器端生成方式

检测目的：对于服务器端生成、由移动终端批量获取的条码生成方式，检查获取的条码是否安全保存，是否与移动终端的唯一标识信息绑定。
检查预生成条码是否定期更换，和采取的保护方式。
获取条码时，后台服务器是否对客户端软件进行身份验证。
检测方法：检查资料说明中预生成条码的保存方式并评估其安全性，以及是否与移动终端的唯一标识信息绑定。

检查设计文档中预生成条码的更换周期，并执行实际测试验证该周期。
检查设计文档中预生成条码的保护方式，是否采取密码技术保护。
尝试从后台服务器获取条码，验证后台服务器存在对客户端软件进行身份验证的过程。

通过标准：对于服务器端生成、由移动终端批量获取的条码生成方式，移动终端客户端软件从后台服务器批量获取预生成的条码，以安全的方式在移动终端上保存。
保存的条码与移动终端的唯一标识信息绑定，防止被非法复制到其他移动终端使用。
预生成的条码定期更换，更新周期宜不超过 24 小时。
采取密码技术对预生成的条码进行保护，防止受到未授权的访问。
从后台服务器获取条码时，后台服务器对客户端软件进行身份验证，防止恶意获取条码。

4.7.2.3 移动终端客户端软件生成方式

检测目的：对于移动终端客户端软件通过生成因子加密动态生成条码的方式，检查条码生成因子的获取途径，保存方式和生成条码的过程，是否与移动终端的唯一标识信息绑定。
检查条码生成因子是否定期更换，以及对其采取的保护方式。

检测方法：检查资料说明中条码生成因子的获取途径，保存方式和生成条码的过程，并评估保存方式的安全性。
检查设计文档中条码生成因子是否与移动终端的唯一标识信息绑定。
检查设计文档中条码生成因子的更换周期，并执行实际测试验证该周期。
检查设计文档中条码生成因子的保护方式，是否采取密码技术保护。

通过标准：对于移动终端客户端软件通过生成因子加密动态生成条码的方式，从后台服务器获取条码生成因子，以安全的方式保存，并通过生成因子加密动态生成条码。
条码生成因子与移动终端的唯一标识信息绑定，防止被非法复制到其他移动终端使用。
条码生成因子定期更换，更新周期宜不超过 7 天。
采取密码技术对生成因子进行保护，防止生成因子受到未授权的访问。

4.8 条码识读与解析

检测目的：检查条码识读时，是否对识读的信息采取了保护措施。
检查条码识别时是否对识读的信息进行了完整性、真实性的校验。
检查条码解析程序自身的健壮性。
检查客户端是否具备识别病毒、木马等恶意代码的能力，是否具备保障交易安全的能力。

检测方法：查看资料说明，确保对条码信息的保密性、完整性、真实性进行了有效的保护方案设计和实现。
通过网络数据抓包、检查是否存在以明文形式传输支付敏感信息。
通过报文重放、报文伪造、使用恶意条码等手段，尝试绕开条码完整性和真实性的校验。

通过标准：条码读取时进行了保密性、完整性和真实性的保障，一般程序无法解析条码信息，无法伪造、篡改交易。
条码解析程序经过漏洞测试、渗透测试、代码扫描等安全检测，具备良好的健壮性。
客户端具备识别病毒、木马等恶意代码的能力。

4.9 交易验证与确认

检测目的：检查所采取的验证要素是否相互独立，验证要素是否符合国家、金融行业标准和相关信息安全管理要求。
检查使用付款扫码时，是否在移动终端界面显著位置展示交易信息，便于客户核对。
检查使用付款扫码时，是否采取了两类或以上要素进行了交易验证。

检查使用付款扫码时，是否由付款人主动发起支付指令，交易信息是否至少包含了收款人信息、金额。

检查使用收款扫码时，是否采取了两类或以上要素进行了交易验证。

检查使用收款扫码时，若在移动终端进行交易验证，是否在移动终端上展现交易信息。

检测方法：查看资料说明，确认在交易验证时采取的验证要素类型。

按照付款扫码流程执行交易测试，观察在交易时，在移动终端界面显示的交易信息内容以及所显示的位置。

按照付款扫码流程执行交易测试，观察在交易过程中，需要使用的验证要素类型。

按照付款扫码流程执行交易测试，观察在交易过程中，是否由付款人主动发起支付指令，交易信息是否包含了收款人信息、金额。

按照收款扫码流程执行交易测试，观察在交易过程中，需要使用的验证要素类型。

按照收款扫码流程执行交易测试，若在移动终端进行交易验证，观察在交易过程是否包含交易信息，如收款人信息和金额。

通过标准：交易验证时：

使用付款扫码时，若采用两种或以上验证要素进行验证，验证要素为客户本人知悉的（如静态密码），客户本人持有的（数字证书、电子签名或一次性密码），用户本人生物特性要素（如指纹等）；若采用不足两类要素验证，应具备相应的风险补偿措施。

使用付款扫码时，交易由客户本人发起，交易信息包含了收款人信息和金额，交易信息在移动终端界面的显著位置清晰展现。

使用收款扫码时，若采用两种或以上验证要素进行验证，验证要素为客户本人知悉的（如静态密码），客户本人持有的（数字证书、电子签名或一次性密码），用户本人生物特性要素（如指纹等）；若采用不足两类要素验证，应具备相应的风险补偿措施。

使用收款扫码时，若在移动终端进行交易验证，交易信息在移动终端界面的显著位置清晰展现。

4.10 交易风险控制

4.10.1 交易风险控制相关信息上送安全

检测目的：检查客户端是否配合业务交易风险控制策略，以安全的方式将相关信息上送至风险控制系统。

检测方法：检查资料说明或开发文档中是否明确要求客户端需上送交易风险控制所需的相关特征信息。

若客户端需上送该类信息，开发文档中应对该类信息进行识别，并就上送策略与安全保护要求进行说明。

若客户端需上送信息用于交易风险控制，则对其上送信息的安全防护机制进行安全性检测。

通过标准：客户端宜配合业务风险控制策略上送有关信息，其信息的处理与传递有一定的安全防护机制，该机制合理、有效。

4.10.2 日累计交易限额验证

检测目的：客户端发起的交易根据不同风险防范能力设置相应的日累计交易限额。

检测方法：检查资料说明中是否明确根据不同风险防范能力设置了相应的日累计交易限额。操作客户端进行交易，验证其日累计交易限额是否有效。

通过标准：使用动态条码进行支付的，风险防范能力及交易限额对应关系如下：

采用包括数字证书或电子签名在内的两类（含）以上有效要素进行验证的。	A 级	可与客户通过协议自主约定单日累计限额

采用不包括数字证书、电子签名在内的两类（含）以上有效要素进行验证的。	B 级	同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 5000 元
采用不足两类有效要素进行验证的。	C 级	同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 1000 元

使用静态条码进行支付的，风险防范能力为 D 级，同一客户单个银行账户或所有支付账户单日累计交易金额应不超过 500 元。

4.11 交易过程安全

4.11.1 交易报文安全

4.11.1.1 交易报文安全

检测目的：检查客户端发起的交易报文能够抗重放攻击、具有抗抵赖性且能被安全地传输。

检测方法：检查评估资料说明或开发文档中防止交易重放攻击的技术手段，并操作客户端进行验证；

检查评估开发文档中保障交易的抗抵赖性的技术手段，包括但不限于交易验证的三类要素，并操作客户端进行验证；

检查评估开发文档中使用的协议，并操作客户端验证是否能够保证交易报文传输安全；

通过标准：客户端报文能够防止对交易的重放攻击，能够保证交易的抗抵赖性，采用了安全协议保证传输安全。

4.11.1.2 交易要素完整性

检测目的：检查客户端发起的交易请求报文中记载的交易要素是否完整。

检测方法：检查资料说明或开发文档对交易请求报文中交易要素的描述，验证客户端发起的交易请求报文中记载的交易要素是否完整；

通过标准：客户端发起的交易请求记载了完整的交易要素。

4.11.1.3 条码识别后的内容安全校验

检测目的：检查客户端能否对条码识别后的内容进行严格的安全校验。

检测方法：检查评估资料说明或开发文档客户端对条码识别后的内容进行安全校验的机制，并操作客户端进行验证。

通过标准：对条码识别后的内容进行严格的安全校验，保证只有合法有效的条码才能进入后续支付流程。

4.11.2 风险识别与干预

4.11.2.1 风险识别

检测目的：检查客户端软件是否能够在交易过程中给予必要的支付风险提示。

检测方法：检查评估资料说明或开发文档中支付风险提示的技术手段，并操作客户端进行验证。

通过标准：客户端应给予必要的支付风险提示，可在每次交易过程中提示，也可在业务开通等环节中提示。

4.11.2.2 风险控制

检测目的：检查客户端软件是否能够配合后台系统对交易过程进行风险识别与干预。
检测方法：模拟风险情况，执行交易，验证客户端软件能够配合后台系统对交易过程进行风险识别与干预。
通过标准：客户端能够配合后台系统对交易过程进行风险识别与干预，防范潜在的非法交易、欺诈交易。

4.11.3 交易监控

检测目的：检查客户端软件是否能够配合后台系统对监控到的风险交易进行处置。
检测方法：检查客户端是否将必要参数传递给风险交易模型以进行风险监控。
通过标准：如风险交易模型涉及到客户端参数，客户端软件应提供参数给监控模型，配合后台系统对监控到的风险交易进行处置。

4.11.4 客户和商户教育

检测目的：检查对客户和商户的教育流程。
检测方法：检查客户端软件的下载渠道。
检查使用说明或其提供的其他途径中关于条码支付的安全知识。
检查向客户提示的安全风险和注意事项。
检查客户适时修改密码的提示。
通过标准：客户和商户教育应通过公开渠道向客户提供安全的包含条码支付功能的客户端程序。
应向客户宣传条码支付的安全知识，提高客户安全防范意识。
应向客户明确提示相关的安全风险和注意事项。应给予必要的支付风险提示，可在每次交易过程中提示，也可在业务开通等环节中提示。
应提示客户适时修改密码。

5 兼容性测试

5.1 显码精度

检测目的：检查客户端软件展示条码时所使用的精度。
检测方法：检查客户端软件展示一维条码和/或二维条码时所使用的精度。
通过标准：客户端软件展示条码时所使用的精度应满足：
被动反射表面：最高表示精度不应超过 0.254mm（10mil），即条码模块的宽度应不小于 0.254mm（10mil）；
主动、半主动发光表面：最高表示精度不应超过 0.381mm（15mil），即条码模块的宽度应不小于 0.381mm（15mil）。

5.2 背光亮度

检测目的：检查客户端软件在展示条码时的亮度。
检测方法：检查客户端软件在展示条码时是否能够自动调节背光亮度。
通过标准：客户端软件在展示条码时能够自动调节背光亮度，且亮度应在100 cd/m^2以上。

5.3 移动终端兼容性

检测目的：检查客户端软件在主流移动终端上的兼容性。
检测方法：将客户端软件安装在主流移动终端上，检查其主要业务功能正常运行。

通过标准：客户端软件的主要业务功能能够在主流移动终端上正常运行。

参 考 文 献

[1] GB/T 12406—2008 表示货币和资金的代码
[2] GB/T 22080—2008 信息技术　安全技术　信息安全管理体系要求
[3] GB/T 22081—2008 信息技术　安全技术　信息安全管理实用规则
[4] GB/T 22239—2008 信息安全技术　信息系统安全等级保护基本要求