# 中国支付清算协会文件

中支协发〔2020〕137号

## 中国支付清算协会关于印发《非银行支付机构预付卡业务风险防范指引》的通知

各预付卡机构:

为防范预付卡条码支付业务风险，引导预付卡机构建立健全预付卡业务风险管理机制，促进预付卡市场规范健康发展，中国支付清算协会组织对《支付机构预付卡业务风险防范指引》（中支协预付卡发〔2013〕4号）进行了修订，更名为《非银行支付机构预付卡业务风险防范指引》，并经中国支付清算协会第三届理事会第二次会议审议通过，现予以发布，自2020年11月1日起施行，请遵照执行。有关事项通知如下:

**一、遵守条码相关技术标准与规范**

预付卡机构发行条码预付卡或依托条码技术受理预付卡支付业务（以下简称预付卡条码支付业务）的，应按照《条码支付安全技术规范(试行)》《条码支付受理终端技术规范(试行)》（银办发〔2017〕242号印发）相关要求，强化预付卡条码支付技术风险防范，加强预付卡条码支付产品安全管理。

**二、严禁超范围从事预付卡业务**

预付卡机构开展预付卡条码支付业务的，应严格按照人民银行核准的业务类型和地域范围开展预付卡业务。通过技术手段确认客户在核准地域范围内，不得借助条码技术超出核准地域从事预付卡业务。未获准办理网络支付业务的预付卡机构不得通过条码技术变相从事网络支付业务。

**三、规范创新业务报告**

预付卡机构拟开展预付卡条码支付业务的，应提前向法人所在地的人民银行分支机构报告。

特此通知。

联系人：王 蕊　童 宁

电　话：010-88665153　88665192

邮　箱：yufuka@pcac.org.cn

中国支付清算协会

2020年9月23日

# 非银行支付机构预付卡业务风险防范指引

（2013年1月23日发布，2020年7月6日修订）

## 第一章　总则

第一条　为促进支付机构预付卡业务健康规范发展，提高支付机构预付卡业务风险防范能力和风险防范水平，根据《支付机构预付卡业务管理办法》（中国人民银行公告〔2012〕第12号）等规章和规范性文件，制定本指引。

第二条　本指引适用于中国支付清算协会开展预付卡业务的会员单位。

第三条　本指引所称支付机构，是指取得《支付业务许可证》，获准办理“预付卡发行与受理”业务的发卡机构和获准办理“预付卡受理”业务的受理机构。

第四条　本指引所称预付卡，是指发卡机构以特定载体和形式发行的、可在发卡机构之外购买商品或服务的预付价值，包括但不限于卡片、密码、条码等形式或载体，载体应符合国家法律法规及监管制度规范有关要求。

第五条　本指引所称条码，是指由一组规则排列的条、空及其对应字符组成的标记，用以表示一定的信息，包括线性条码、二维条码等。

支付机构可以通过手机客户端或相关载体发行条码形式的预付卡，可以通过在特约商户布放受理终端或收款码等方式受理

本机构或合作机构发行的预付卡。

第六条　本指引所称预付卡业务风险是指支付机构在开展预付卡业务活动中，即在发行、受理、资金结算、系统运维等方面，遭受负面影响和损害的可能性。

第七条　本指引所称预付卡业务风险防范是指支付机构在开展预付卡业务时，进行风险监控、风险识别、风险评估、风险应对等一系列活动的总称。

（一）风险监控是指以人工监控和系统监控为主要手段，针对可能出现风险的环节、岗位、系统、资金等方面进行全面监测和控制；

（二）风险识别是指根据业务流程和业务特点确定重点关注的事项，及时发现风险隐患；

（三）风险评估是指针对风险隐患可能产生的后果和危害程度进行分析和评价；

（四）风险应对是指针对风险评估结果采取相应措施。

第八条　预付卡业务风险防范的目标：

（一）确保预付卡业务风险控制在本机构可承受范围内；

（二）确保本机构遵守法律法规或有关规定，依法合规开展预付卡业务，未获准办理网络支付业务的发卡机构不得通过条码变相从事网络支付业务；

（三）确保本机构预付卡业务的安全性、连续性、可控性，提高经营效率；

（四）确保本机构建立重大风险应对措施，避免机构遭受重大损失。

第九条　风险防范的基本要求：

（一）支付机构的预付卡业务各环节应严格遵守国家相关法律法规及相关制度，加强内部监督检查，依法合规经营，防范违法、违规风险；

（二）利用人工、系统等手段对预付卡业务进行全流程、全时段、全方位监控，避免出现遗漏；

（三）支付机构相关内设部门应对各业务环节进行监控，及时识别、评估各类风险的危害程度，并及时采取应对措施；

（四）支付机构应加强风险防范意识，积极采取有效手段，不断提高风险防范水平；

（五）加强支付机构从业人员职业操守、业务能力的教育和培训，不断提高从业人员的业务素质和职业道德水平。

## 第二章　发行环节的风险防范

第十条　发行环节的风险包括卡片制作及条码生成风险、库存风险、意外风险、操作风险等。

第十一条　卡片制作风险是指由于制卡厂商资质不符合相关标准，卡片信息在生成过程中不符合相应规范，卡片信息泄露，或因制卡厂商违约等情况导致的风险。条码生成风险是指条码信息生成过程中由于不符合相应规范或条码信息泄露等情况导致

的风险。

风险识别应重点关注以下事项：

（一）制卡厂商是否具备相应资质；

（二）制卡厂商的卡片信息保护措施；

（三）卡片信息在生成过程中是否符合相应规范；

（四）制卡信息传输的安全与保密；

（五）制卡信息在制卡后的销毁时限与操作规范；

（六）采购协议的履行情况；

（七）卡片封装和验收；

（八）条码生成是否符合国家相关标准或规范。

第十二条　卡片制作及条码生成风险的评估与应对：

该类风险可能导致卡片的编码规则被破译，卡片被伪造或变造；条码中被植入木马、病毒造成客户信息泄露和资金损失的风险；或由于制卡厂商出现违约情况等影响本机构正常业务开展。支付机构应从风险事件的性质、程度和范围，涉及的卡片及条码数量和资金额度，对本机构业务开展的影响程度等方面进行评估。

（一）严格遵守有关制卡的相关规定，选择风险控制符合规范的制卡厂商，支付机构发行的预付卡在受理时与银行卡共用机具的，应选择具有银行卡制作资质的制卡厂商；

（二）严格考察预付卡制卡厂商的能力、资质、诚信，审慎选择取得行业相关认证的正规制卡厂商，并签订采购协议；

（三）卡片生成信息应符合相应的技术规范，确保存储介质的唯一性；

（四）制卡厂商应在制卡后三日内销毁制卡信息，并有相应操作规范；

（五）严格执行采购协议中的信息保密条款，相关信息采用密文传输、密文存储，制卡时覆膜保证初始密码的安全；

（六）按照内部控制制度，保证采购流程有序进行；

（七）对有分支机构或分公司的发卡机构，应由总公司统一负责卡片采购；

（八）生成预付卡条码的软硬件应使用经国家密码管理机构认可的密码产品；

（九）支付机构在预付卡发行环节存在同一预付卡多种载体形式需求的，需在发行时与客户明确约定卡片、条码等不同载体是否兼容，并设置相应的风险监测、防控机制，及时识别可疑的兼容交易，采取相应风控措施；

（十）发行条码预付卡的支付机构应明确业务风险点及相关责任承担机制、风险损失赔付方式及操作方式，并应开展对客户的条码支付安全教育，提升其风险防范意识和应对能力。

第十三条　库存风险是指由于岗位设置不完善、制度执行不严格造成卡片丢失、损毁，或因卡片丢失引发信息泄露导致的风险。

风险识别应重点关注以下事项：

（一）库存保管制度的落实情况；

（二）库存盘点是否账实相符。

第十四条　库存风险的评估与应对：

该类风险可能导致卡片丢失、损毁，进而影响售卡业务的开展，或因卡片丢失导致卡片被伪造、变造。支付机构应从风险事件的性质、程度和范围，涉及的卡片数量及资金额度，对本机构业务开展的影响程度等方面进行评估。

（一）库存保管岗位应专人专岗，双人复核；

（二）严格执行卡片保管制度、出入库管理制度；

（三）对卡片的领用、售出和结存情况按公司制度定期进行盘点；

（四）针对盘点中发现的问题或差错，及时采取措施。

第十五条　意外风险是指卡片在保管、配送、销售过程中发生意外情况导致的风险。

风险识别应重点关注以下事项：

（一）卡片保管、销售场地的安保措施；

（二）卡片配送过程的安全；

（三）其他意外事件。

第十六条　意外风险的评估与应对：

该类风险可能导致因卡片丢失、被盗、消磁等直接影响业务开展与客户的正常使用。支付机构应从风险事件涉及的卡片数量、客户数量、销售网点或区域，对本机构业务开展的影响程度，

补救周期等方面进行评估。

（一）在卡片库存区域、销售区域设置摄像监控、紧急报警系统、保险柜等；

（二）在卡片同城或异地配送过程中，应采取必要的安保措施；

（三）做好安全记录，制定应急预案并定期进行检查及演练；

（四）购买保险、设置发生意外时责任归属的合同条款等；

（五）发生意外情况时，应按照应急预案及时采取应对措施。

第十七条　操作风险是指售卡过程中，相关人员因操作失误等情形导致的风险。

风险识别应重点关注以下事项：

（一）账实是否相符；

（二）卡片实售数量、金额与应售数量、金额是否一致；

（三）相关人员的业务能力和职业道德；

（四）是否有已离职人员、岗位调整人员或不相关人员拥有售卡权限；

（五）售卡环节的信息安全；

（六）发票的开具是否符合税务机关规定。

第十八条　操作风险的评估与应对：

该类风险可能导致售卡金额与实际收取的金额不符、卡片实售数量与应售数量不符、本机构业务信息与客户信息泄露等，进而影响业务正常开展与客户正常消费。支付机构应从风险事件发

生的频次和岗位，涉及的资金额度，涉及信息的性质、程度和范围，客户投诉量，对本机构声誉的影响程度等方面进行评估。预付卡机构发行可在公共交通领域使用的预付卡的，可参照相关法律法规另行规定。

（一）严格制定售卡操作流程，做好值班登记，业务系统日志应完整记录所有操作记录；

（二）加强相关人员培训，提高业务能力；

（三）售卡计算机应设置密码口令并定期更改，确保专人专用，登录售卡计算机应采取至少 2 个要素进行操作人员的信息验证，要素验证方法包括但不限于密码验证、UKEY 和手机短信验证等；

（四）售卡计算机不得外接移动存储介质，不得接入互联网；

（五）加强重要岗位人员的操作复核和监督，防范道德风险，在涉及持卡人权益的业务操作流程中应设立至少 2 个不同操作权限的操作岗位；

（六）严格审核并控制售卡人员权限开立，每年定期组织操作人员账户权限清查及调整工作；

（七）对业务开展中发现的问题，视情况采取相应处理措施；

（八）根据税务相关政策规定，按合适科目开具发票，不得虚开发票。

## 第三章　受理环节的风险防范

第十九条　受理环节的风险包括商户资质风险、商户拓展中的操作风险、商户合作中的法律风险、商户欺诈风险、异常交易风险、可疑交易风险等。

第二十条　商户资质风险是指由于特约商户的资质不符合相关规定导致的风险。

风险识别应重点关注以下事项：

（一）是否为禁止发展类商户，包括非法设立的商户；赌博及博彩类、色情服务类，出售违禁药品、毒品、黄色出版物、军火弹药以及其他与国家法律、法规相抵触的商户；互联网销售彩票平台，非法外汇、贵金属投资交易平台，非法证券期货类交易平台，代币发行融资及虚拟货币交易平台，未经监管部门批准通过互联网开展资产管理业务以及未取得省级政府批文的大宗商品交易场所等商户；停业整顿、濒临破产或已破产的商户；注册地及经营场所不在中国境内的商户；商户、商户法人代表或其主要负责人涉及重大民事纠纷或涉嫌犯罪并严重影响商户正常经营的；

（二）是否为谨慎发展类商户，包括易发生风险的商户，如：机票代售点或手机专卖店；黄金销售类商户；各类娱乐场所，如夜总会、卡拉 OK 、酒廊等；电话购物、邮购及网购商户；提供中介、咨询类服务的商户；批发类商户，包括专业化批发市场、小商品市场等；实际销售的商品或提供的服务不明确的商户，如小型贸易公司、经贸公司等；被其他支付机构拒绝签约或撤销的

商户；

（三）是否为重点识别类商户，包括缺少经营情况辅助证明材料的市场摊位、临时性销售点、流动摊贩等小微商户。

第二十一条　商户资质风险的评估与应对：

该类风险可能导致直接违反国家法律法规或相关规定，也可能因商户出现意外情况，导致客户无法正常消费。支付机构应从风险事件的性质，对客户的影响程度，对本机构声誉的影响程度等方面进行评估。

（一）深入细致进行现场考察；

（二）严格执行商户拓展制度，严格审核商户资质；

（三）严格履行签约流程并妥善保存商户信息资料。

第二十二条　商户拓展中的操作风险是指业务人员在与特约商户签约过程中出现违规操作导致的风险。

风险识别应重点关注以下事项：

（一）业务人员是否有泄露本机构和特约商户商业秘密的情形；

（二）业务人员是否有违反道德规范损害本机构利益的情形：包括与特约商户联合伪造资质、明知或应知商户涉嫌违规但仍为其提供协助等；

（三）业务人员是否核实小微商户经营辅助证明材料；

（四）业务人员是否严格遵守商户拓展的审批流程。

第二十三条　商户拓展中操作风险的评估与应对：

该类风险可能导致本机构和特约商户利益受损等。支付机构应从风险事件的性质、程度和范围，对本机构和特约商户利益的影响程度等方面进行评估。

（一）与相关操作人员签署保密协议，保守商业秘密；

（二）落实岗位责任制，明确责任人；

（三）严格签约流程和审批程序，妥善保管签约资料；

（四）定期采取抽查资料、实地考察等方式对签约商户进行核查，发现问题后及时采取相应措施。

第二十四条　商户合作中的法律风险是指与特约商户签订的合作协议、合同条款出现法律纠纷，或因特约商户违约导致的风险。

风险识别中应重点关注以下事项：

（一）合同条款的合法性；

（二）因商户违约产生的法律纠纷。

第二十五条　商户合作中法律风险的评估与应对：

该类风险可能导致本机构在法律纠纷中处于被动地位，利益和声誉受到损害。支付机构应从风险事件涉及的合法性缺失的性质与程度，对本机构利益和声誉的影响程度等方面进行评估。

（一）设立法律顾问岗位或聘请相应的法律专业人员；

（二）审核合作协议、合同条款的合法性；

（三）规范预付卡受理的协议条款，明确商户不得歧视和拒绝使用卡片及条码支付的客户；

（四）对可能产生的法律纠纷制定相应防范措施；

（五）对已产生的法律纠纷，及时提出解决方案，保障机构和客户的合法权益。

第二十六条　商户欺诈风险是指特约商户为获取利益，故意采用非法或者非正常的市场行为扰乱市场秩序导致的风险。

风险识别应重点关注商户是否有以下行为：

（一）明知持卡人进行洗钱、赌博等犯罪活动而提供支付服务；

（二）虚假申请受理终端或收款码后进行欺诈活动，或转卖、转租、转借机具或收款码提供给不法分子使用；

（三）违规留存、泄露、转卖预付卡交易信息，或默许纵容不法分子盗取预付卡交易信息；

（四）用虚构交易、虚开价格、现金退货等方式为持卡人提供预付卡套现服务；

（五）在持卡人不知情的情况下，编造虚假交易或重复交易盗取资金。

第二十七条　商户欺诈风险的评估与应对：

该类风险可能导致本机构在不知情的情况下为非法活动提供服务进而使本机构利益和声誉受到影响，还可能导致客户合法权益受到损害。支付机构应从风险事件的性质、程度、持续时间，涉及的资金额度和客户数量，对本机构利益和声誉的影响程度等方面进行评估。

（一）落实商户分级审批制度，对发生欺诈行为的特约商户，列为高风险等级商户或禁止合作商户，出现第二十六条情形的，应取消特约商户资格，其他支付机构不得将其发展为特约商户；

（二）严格执行特约商户管理制度，采取定期、不定期的形式对特约商户进行巡检，及时发现可能存在的问题；

（三）要求特约商户对检查中出现的问题进行限期整改，必要时终止合作；

（四）对商户就卡片受理及条码支付受理等进行风险培训，明确界定商户违规操作行为及相关责任，并建立相应的回访机制。

第二十八条　异常交易风险是指客户采取伪造、变造预付卡或条码等手段非法获取利益导致的风险。

风险识别应重点关注以下情形：

（一）单个受理终端出现多次报警；

（二）多个受理终端出现报警。

第二十九条　异常交易风险的评估与应对：

该类风险可能直接导致本机构和客户的利益受损。支付机构应从风险事件发生的区域、持续时间，涉及的终端数量、商户数量、资金额度和客户数量等方面进行评估。

（一）系统应具备卡片状态查验功能，状态正常时方可允许交易，非正常时发出错误警示；

（二）系统应限定错误密码的输入次数，错误密码输入超过

一定次数时，及时自动锁卡；

（三）设置异常交易监测岗位，对出现错误警示的交易情形和错误警示发生率较高的特约商户进行跟踪监测，分析并评估相应风险，及时采取应对措施；

（四）支付机构应能够有效识别本机构发行的客户端程序和布放的特约商户受理终端、收款码，能够确保条码生成和识读过程的安全性，规避交易风险；

（五）支付机构可根据条码支付场景不同，如静态条码、动态条码等，合理评定条码支付特约商户的风险等级，根据风险程度设置不同的条码支付限额、所需验证要素等；

（六）预付卡条码受理终端须满足国家相关规范，防范设备硬件不达标可能产生的交易风险；

（七）预付卡条码支付的交易报文等应遵守国家相关技术规范，保障交易信息的一致性、完整性及安全性。

第三十条　可疑交易风险是指客户为获取利益，单独或与特约商户合作进行洗钱、恐怖融资导致的风险，以及倒卖预付卡并通过虚假交易套现的风险。

风险识别应重点关注以下情形：

（一）单个商户持续大额交易，或在短时间内发生大额集中交易，且与平时交易差别较大；

（二）非正常赎回；

（三）可疑客户或机构的大批量持续性消费、充值或大批量

异地消费;

（四）可疑客户或机构以相同、整数或倍数金额消费或充值;

（五）多个终端存在关联卡交易且多次触发监控;

（六）预付卡在网络渠道发生大额或者高频的购买虚拟商品交易。

第三十一条　可疑交易风险的评估与应对:

该类风险可能直接导致本机构在不知情的情况下为违法行为提供服务。支付机构应从风险事件发生的频次，涉及的资金额度和商户数量，对本机构声誉的影响程度等方面进行评估。

（一）严格执行国家反洗钱、反恐怖融资的有关规定;

（二）严格按照国家反洗钱、反恐怖融资规定的要求对可疑交易进行实时监控;

（三）对可疑交易行为及时按规定要求上报;

（四）对可疑交易涉及的客户信息及账户信息妥善保管;

（五）根据国家有关部门要求，配合执法部门的调查、取证及处理工作。

## 第四章　资金结算的风险防范

第三十二条　资金结算风险是指因支付机构与特约商户结算时出现差错，或支付机构结算操作人员虚构结算对象、支付机构系统被不法分子入侵发出伪冒资金指令等，给资金安全带来隐患导致的风险。

风险识别应重点关注以下事项:

（一）与特约商户对账是否存在差异;

（二）与清算机构对账是否存在差异;

（三）是否与特约商户就差错处理的有关事项进行明确约定;

（四）对于系统资金清结算系统自动化程度较高的机构，当出现系统异常、网络延迟等情况时，是否存在商户资金重复结算的可能;

（五）资金结算对象是否为实际开展合作的特约商户或具有实际业务背景，资金结算指令中收款账户信息是否真实、准确。

第三十三条　资金结算风险的评估与应对:

该类风险可能导致本机构与特约商户无法正常结算，或结算资金被挪用，影响客户的正常消费。支付机构应从风险事件发生的性质和频次，涉及的商户数量、资金额度和操作人员等方面进行评估。

（一）与特约商户事先约定结算事项、结算周期与差错处理办法;

（二）严格执行与特约商户、清算机构的对账机制，及时发现差错并进行相应处理;

（三）妥善保管差错处理环节中产生的相关资料;

（四）如出现系统异常、网络延迟等情况，机构需停止资金结算相关操作。网络恢复正常后，机构需进一步核查自身账户状

态，确认无误后再执行资金结算操作；

（五）对资金结算操作严格执行经办、复核管控，加强对操作人员的内控检查及职业道德教育。

## 第五章　系统运维的风险防范

第三十四条　系统运维风险是指因系统遭受外部攻击导致的风险，或因异常原因造成系统非正常中断，影响预付卡业务正常开展的风险。

风险识别应重点关注以下事项：

（一）机房环境及安全措施；

（二）系统硬件环境及安全措施；

（三）系统软件配置及安全措施；

（四）系统在遭受攻击或发生不可抗力灾害情况下的应急措施。

第三十五条　系统运维风险的评估与应对：

该类风险可能导致存储信息被篡改或被盗、业务系统瘫痪，造成预付卡业务非正常中断，影响客户的正常消费和资金、信息安全等。支付机构应从风险事件的性质，涉及的信息数量和资金额度，系统中断时间长短，对客户的影响程度和对本机构业务开展的影响程度等方面进行评估。

（一）做好机房安全保障工作，包括机房场地保障、机房环境保障、网络保障、电力保障、安全保障、消防保障和技术支持

保障；

（二）采用容量大、容错性高的系统，支持巨量卡片的发行和交易处理，保障交易成功率；

（三）采取必要的加密技术，防止交易数据在传输、存储过程中被截取、修改或丢失，对数据的完整性、一致性、安全性进行控制管理；

（四）加强网络安全控制，禁止不安全协议访问系统主机；

（五）定期进行系统抗攻击能力测试，检查防火墙和网关，及时升级防病毒软件和更新补丁；

（六）在硬件、操作系统、应用、数据库等层次采用相应的冗余技术和恢复策略，具备灾难恢复处理能力和应急处理能力；

（七）对系统的运行情况进行实时监控，及时发现攻击行为或存在的安全隐患，并做出快速反应；

（八）制定突发事件应急预案，建立灾难备份系统，确保预付卡业务，包括条码预付卡业务的连续性和业务系统安全运行；

（九）当系统出现异常情况发生中断时，及时启动应急预案，按规定要求采取相应措施。

## 第六章　附则

第三十六条　有关客户权益保护环节的风险防范可参照《支付机构预付卡业务客户权益保护指引》，本指引未作规定的其他业务风险，支付机构应参照本指引的有关要求，制定相应的风险

防范措施。

第三十七条　国家法律、法规及部门规章对预付卡业务风险防范另有规定的，从其规定。

第三十八条　本指引由中国支付清算协会负责解释。

第三十九条　本指引自2020年11月1日起施行。

内部发送：协会秘书处。

中国支付清算协会秘书处　　2020年9月23日印发