**中国银行业协会关于落实银行与第三方支付机构合作管理的操作指引**

**关于落实银监发〔2014〕10号文要求的操作指引**

为贯彻《中国银监会中国人民银行关于加强商业银行与第三方支付机构合作业务管理的通知》(银监发〔2014〕10号，以下简称《通知》)要求，落实商业银行客户金融信息管理职责，做好客户信息安全与保密工作，现根据《通知》要求形成操作指引，具体内容说明如下：

第一条 商业银行是客户金融信息管理方，客户身份信息与银行账户信息应由商业银行统一管理。商业银行与第三方支付机构合作业务中(包括但不限于网关支付、快捷支付、无磁无密支付、信用卡还款等)，应确保业务开展各环节的客户信息和账户信息留存银行，不得违反相关法律法规和监管制度要求泄露信息，并应根据客户实际意愿和操作指令完成账户关联或资金划付。

第二条 第三方支付机构是指依法取得《支付业务许可证》，获准办理互联网支付、移动电话支付、固定电话支付和数字电视支付等网络支付业务的非金融机构。

第三条 商业银行应构建客户风险政策管理体系，根据客户个人风险承受能力(包括不限于年龄、学历、职业、消费习惯、是否有网络支付经验、是否了解网络支付风险等)与业务风险承受能力(包括不限于账户状态、交易类型、交易频次等)综合判断客户是否适宜开展各类合作业务，同时商业银行应根据上述综合风险承受能力建立客户风险评级制度，根据不同风险等级细化客户开展各类业务的条件与适宜开展的业务内容，包括但不限于允许关联第三方支付机构账户数、允许开通的交易种类(如消费(含预授权交易)、代收、代付、缴费、转账等)等。

第四条 商业银行应制定通过第三方支付机构的单笔、日累计交易限额，银行设定或客户主动申请调整该交易限额的，应根据客户实际风险承受能力进行合理评估。建议单笔交易限额初始金额2000元，最高不超过5000元，日累计交易限额初始金额5000元，最高不超过20000元，各商业银行实际执行中可根据业务情况酌情调整。

第五条 确系业务需要，客户银行账户与第三方支付机构账户建立一次签约、多次支付的业务关系的，在两账户首次建立业务关联时，商业银行应要求第三方支付机构以书面协议方式获取客户授权并落实自身客户身份验证工作，协议中应明确第三方支付机构对于客户实名制账户开立、认证的独立责任归属。

第三方支付机构完成自身客户身份验证后，应要求客户跳转至银行界面完成客户银行账户的身份验证与签约，并上送客户姓名与支付账户作为必要信息至银行进行业务关联申请。银行应书面协议方式获取客户同意，对银行账户与第三方支付机构账户建立一次签约、多次支付的业务授权，并落实客户身份验证。对于在银行界面通过身份验证的，允许其银行账户与第三方支付机构账户建立唯一对应关系。

商业银行与第三方支付机构客户身份验证工作应保持独立性，不得互串互验。商业银行不得对于第三方支付机构收集的客户身份验证信息和账户信息进行验证。

商业银行与第三方支付机构应落实各自验证责任，对于未落实验证责任或存在验证错误的一方应承担由此导致的交易参与各方的风险损失。商业银行在落实前述银行账户与第三方支付机构账户关联要求的前提下，后续支付交易中，可根据自身风险控制要求自行选择是否仍需要对客户身份信息进行再次验证。对于未与第三方支付机构账户建立业务关联并直接通过银行账户进行支付的，商业银行应确保客户逐笔交易均跳转银行渠道(含银行界面渠道与银行语音渠道)进行客户身份验证，验证通过的方能进行交易授权。

第六条 商业银行应遵循双(多)因素验证方式进行客户身份验证，身份认证由至少两种身份认证方式组成：一是客户知晓、注册的客户名称及密码(如姓名、用户名、身份证号、信用卡有效期、取现密码等);二是客户持有、特有并用于实现身份认证的信息，包括但不限于物理介质或电子设备等(如手机动态验证码、USB Key等)。如不具备上述要求的，不允许建立与第三方支付机构业务关联。对于通过手机动态验证码进行验证的，应由发卡银行发送并完成验证，不得委由第三方支付机构或其他任何机构代发代验。

第七条 商业银行应开通至少一种账户变动通知方式(如：邮件、短信、微信、图片、语音等)对银行账户与第三方支付机构账户建立关联的客户进行即时告知，如不具备上述要求的，不允许银行账户与第三方支付机构账户之间建立业务关联及进行后续资金划付。

第八条 对于支付类业务，商业银行应要求第三方支付机构落实二级商户编码唯一性，准确标识并完整上送交易信息，至少应包括：直接提供商品或服务的二级商户名称、类别和代码、受理终端(网络支付接口)类型和代码、交易时间和地点(网络特约商户的网络地址)、交易金额、交易类型和渠道、交易发起方式等，网络特约商户的交易信息还应当包括商户订单号和网络交易平台名称。同时银行应制定规范化标准接口实现统一接入，并要求所有合作的第三方支付机构经过监管机构认证的证书对其发起交易签名，保障传输信息的完整性、一致性和不可抵赖性。

第九条 商业银行应加强大额支付、可疑支付资金划转监控与管理，通过短信或其他方式及时通知客户相关信息，包括但不限于第三方支付机构名称、提供直接服务或商品商户名称、交易金额、交易时间等，以确保该支付指令系客户本人真实意愿反映。

第十条 商业银行应提供客户撤销客户银行账户与第三方支付机构账户关联关系的服务，同时应与第三方支付机构同步双方账户解约信息，对于撤销关联关系后的交易将无法适用原有交易验证流程进行授权。对于通过银行发起的撤销关联关系申请，银行应及时在系统中予以记录并通知第三方支付机构且立即对于后续所有借记交易予以拒绝;对于通过第三方支付机构发起的撤销关联关系申请，银行应在获取第三方支付机构解约信息后及时在系统中予以记录，并对于后续所有借记交易予以拒绝。

如客户撤销关联关系后需要重建关联关系的，对于客户通过第三方支付机构发起重建关联关系的申请，银行应要求第三方支付机构按照新建立业务关联要求落实客户身份实名制验证并跳转至银行界面再次进行客户身份验证;对于客户通过银行发起的重建关联关系申请，银行应落实客户身份验证并同步信息到第三方支付机构。

第十一条 商业银行应至少通过一种渠道向客户提供签约查询与交易查询功能，并在法律法规规定期限内妥善保管完整支付信息以备核查，包括客户银行账户与第三方支付机构账户建立关联信息、撤销账户关联信息、客户通过第三方支付机构关联账户完成支付具体交易信息(含提供直接服务或商品商户名称、交易金额、交易时间)等。

第十二条 商业银行应加强支付交易资金管理，严格按照备付金管理办法监管要求与第三方支付机构开展相关业务。

商业银行对于从银行账户中划付的支付交易资金如遇交易终止、失败的，应按照“从哪来回哪去”原则，返回划出的银行账户，不得留存第三方支付机构的支付账户中。

第十三条 商业银行应通过协议等文本形式与第三方支付机构就合作业务中双方权利义务责任达成共识，包括但不限于：第一，落实第三方支付机构因开展一次关联多次支付业务产生的所有风险交易责任归属;第二，落实第三方支付机构通过银行认可模式完整上送交易信息的责任;第三，落实第三方支付机构承担批量扣款类非经商业银行直接进行客户身份认证支付的交易责任(如有);第四，落实第三方支付机构不得未经允许屏蔽银行支付界面和接口的责任;第五，落实因第三方支付机构信息泄露引发各支付渠道风险交易的责任，以确保双方业务开展合规性。

第十四条 商业银行应进一步构建并完善业务风险监控与管理体系，加强与第三方支付机构合作业务管理，做好客户交易资金与可疑商户资金实时监测、核查、预警、控制，有效化解支付业务潜在风险。

第十五条 商业银行应在确保客户信息安全的前提下，要求第三方支付机构通过银行认可模式(如：专网专线等)进行数据信息传输，同时应构建安全防火墙并设定有效隔离区，防止第三方支付机构进行越界访问。

第十六条 商业银行应通过不同渠道尤其是银行自有渠道(包括但不限于短信、账单、微信、邮件等多种方式)加大客户教育力度，强化客户通过第三方支付机构通路进行交易的风险隐患认知，提高自身信息安全与风险防范意识。

第十七条 商业银行应按照本指引要求，做好相应业务梳理与整改工作。制度及合同修订工作应于2014年10月31日前完成，系统改造工作最迟应于2014年12月31日前完成。自2014年11月1日起，商业银行与第三方支付机构新开展业务合作应按照本指引要求执行，存量业务协议应在2014年10月31日前完成重新签署。

商业银行对于已合作第三方支付机构且已建立业务关系的客户应通过双方数据移植等方式一次性落实双方账户关联，并要求第三方支付机构及时销毁留存所有存量客户涉密信息(包括姓名、卡号、身份证号、信用卡有效期等)。

第十八条 各商业银行应建立自查自纠机制，每年就相关执行情况开展检查，每半年将检查结果及时反馈中国银行业协会银行卡专业委员会，中国银行业协会将就执行情况及时报告监管部门。

第十九条 本指引自下发之日起执行，各项条款解释与修订工作归属中国银行业协会银行卡专业委员会。