ICS 35.240.40
A11

团 体 标 准

T/PCAC：0001-2023

个人支付信息保护指引

Guidelines for personal payment information protection

2023-08-03 发布 2023-08-03 实施

中国支付清算协会发布

目 录

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 T/PCAC 0001—2016《个人信息保护技术指引》，T/PCAC 0001—2016 相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改标准范围为个人支付信息，并给出个人支付信息的分类（见 6.1）；

——提出了个人支付信息安全框架（见 8）；

——明确了支付业务主体开展个人支付信息保护时的基本范围（见 9）；

——针对性提出不同角色的支付业务主体的基本要求（见 10）；

——提出了从业机构的管理要求（见 11）；

——提出了从业机构的人员要求（见 12）；

——提出了从业机构的系统要求（见 13）；

——针对不同场景提出了个人信息保护的典型要求（见 14）。

本文件由中国支付清算协会提出。

本文件由中国支付清算协会安全与技术标准专业委员会归口。

本文件起草单位：中国支付清算协会、北京国家金融科技认证中心有限公司、中金金融认证中心有限公司、北京银联金卡科技有限公司、北京软件产品质量检测检验中心、网银在线（北京）科技有限公司、财付通、通联支付、中国银联股份有限公司、网联清算有限公司、Visa、中国工商银行、浙江大学滨江研究院。

本文件主要起草人：陈波、潘松、左泽华、侯玉华、相海飞、高展、张海燕、李振、李博文、郭大圣、张健、李作全、马鸣、于柳绮、张大健、王波、王宏铭、姚乾、郑峥、李宇、王威、张鹏、翟耀超、高卓、邵晓博、吴永强、程虎、蒋增增、石常蕴、王维、赵刚、陈俊、邹元、崔凌、杜志琴、韩蒙。

本文件及其所替代文件的历次版本发布情况为：

——2016 年首次发布为 T/PCAC 0001—2016，本次为第 1 次修订。

引　言

为进一步规范个人支付信息处理活动，本指引结合支付业务的参与主体和业务特点，在符合国家及行业监管要求，遵循 GB/T 35273、JR/T 0171 等标准规范的基础上，提出了支付信息保护整体框架，细化了支付业务中个人信息的处理要求和相关机构的能力要求，为参与支付业务的机构提供指导。

个人支付信息保护指引

1 范围

本规范给出了个人支付信息的范围定义，提出了个人支付信息保护的基本原则、安全框架、安全保护范围、业务主体及主要义务、组织建设、人员管理、终端和业务系统安全等内容，并针对不同业务场景提出了典型的保护要求。

本规范用于指导本协会会员单位信息系统处理个人支付信息的服务与活动。

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/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0197—2020 金融数据安全 数据安全分级指南

T/PCAC 0003—2018 银行卡销售点（POS）终端检测规范

T/PCAC 0005—2019 条码支付受理终端检测规范

3 术语和定义

GB/T 35273—2020 及 JR/T 0171—2020 界定的以及下列术语和定义适用于本文件。

3.1 个人信息 personal information

以电子或者其他方式记录的、能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[GB/T 35273—2020,定义 3.1]

3.2 个人支付信息 personal payment information

在支付服务过程中获取、加工和保存的个人信息。

3.3 支付业务主体 payment service institution

从事支付业务、处理个人支付信息的服务机构，包含收单机构、账户机构、清算机构和其它相关机构。

3.4 个人支付信息环境 personal payment information environment

个人支付信息环境由以下部分组成：

- 存储、处理或传输个人支付信息的系统组件、人员和流程；
- 可能不存储、处理或传输个人支付信息的系统组件，但它们可以不受限制地连接到那些存储、处理或传输个人支付信息的系统组件。

3.5 系统组件 system components

包含在或连接到个人支付信息数据环境或可能影响个人支付信息数据环境安全的任何网络设备、服务器、计算设备或应用程序。

4 缩略语

CVN(Card Verification Number) / CVN2(Card Verification Number 2) 卡片验证码

SIEM(Security Information and Event Management) 安全信息和事件管理

NTP(Network Time Protocol) 网络时间协议

DNS(Domain Name System) 域名系统

5 编制原则

--与时俱进原则。遵循《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等最新法律法规，符合国家及行业监管要求，并与前沿的数据安全研究充分结合。

--行业适用性原则。突出支付属性，从支付领域典型业务场景切入，紧密围绕支付业务模型编制，聚焦个人支付信息流转链条，吸纳业界成熟的信息处理管理及技术方案。

--技术包容性原则。在提出个人支付信息保护实施建议的同时，允许机构在技术发展的前提下不断创新，经验证有效的创新技术手段将迭代纳入本指引。

6 个人支付信息分类分级

6.1 个人支付信息分类

个人参与支付活动中涉及的、能够被知晓和处理、与个人相关、能够单独或与其他信息结合识别该个人的任何信息：

a) 账户信息指账户及账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等；

b) 鉴别信息指用于验证主体是否具有访问或使用权限的信息，包括但不限于银行卡密码、预付卡支付密码；个人支付信息主体登录密码、账户查询密码、交易密码；卡片验证码（CVN 和 CVN2）、动态口令、短信验证码、密码提示问题答案等；

c) 支付交易信息指个人支付信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、透支记录、交易日志、交易凭证；

d) 个人身份信息指个人基本信息、个人生物识别信息等：

- 个人基本信息包括但不限于客户法定名称、身份证和护照等证件类信息、联系方式（如手机号码、固定电话号码、电子邮箱），以及在提供产品和服务过程中收集的照片、音视频等信息；
- 个人生物识别信息包括但不限于指纹、人脸、虹膜、耳纹、掌纹、静脉、声纹、眼纹、步态、笔迹等生物特征样本数据、特征值与模板。

e) 其他信息：

- 对原始数据进行处理、分析形成的，能够反映特定个人某些情况的信息，包括但不限于特定个人支付信息主体的消费意愿、支付习惯和其他衍生信息；
- 在提供支付服务过程中获取、加工、保存的其他个人信息。

6.2 个人支付信息分级

个人支付信息分级参考 JR/T 0171—2020 和 JR/T 0197—2020 执行。

7 个人支付信息处理基本原则

个人支付信息的处理遵循 GB/T 35273—2020 及 JR/T 0171—2020 的基本原则。

8 个人支付信息安全框架

个人支付信息安全框架如图 1 所示。

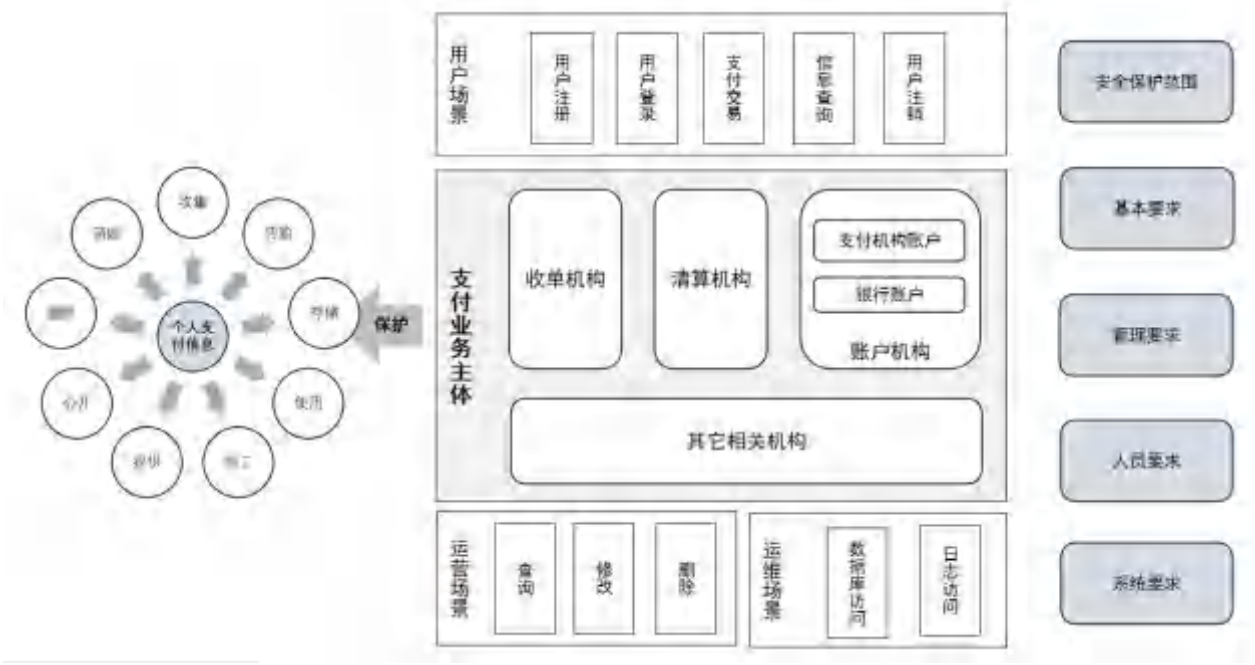

图 1 个人支付信息安全框架

个人支付信息在支付业务中，需要在不同支付业务主体之间流转。个人支付信息的生命周期与支付业务主体、业务场景、支付技术的选择有密切关系。因此，在本支付框架中提出 3 项要素：

a） 支付业务主体：宜按照处理支付信息的主要类别开展信息保护工作，甄别各类支付业务主体的主要职责，确定自身的安全保护范围，并按照基本要求、管理要求、人员要求、系统要求等不同的维度建立个人支付信息保护能力；

b） 业务场景：个人支付信息保护需要实现场景的全覆盖。根据支付服务参与角色的不同，至少需要考虑用户场景、业务运营场景、系统运维场景的数据保护；

c） 支付技术：宜根据支付技术的不同设定具体的个人支付信息保护要求，包括网络支付、移动支付、银行卡收单等不同的技术模式。

个人支付信息的生命周期包括收集、传输、存储、使用、加工、提供、公开、删除、销毁等。

a） 收集是个人支付信息中外源性信息的主要来源。通过移动 App 等智能终端进行信息采集时，宜符合 GB/T 41391—2022 的要求；通过其他非信息化系统收集个人信息时，遵循 GB/T 35273—2020、JR/T 0171—2020 中信息收集的基本原则，特别需要注意纸质文件扫描或通过 OCR 等方式转化为电子数据的过程；

b） 个人支付信息在不同参与主体之间传输时，宜采用加密通道、数据加密的方式保障数据安全性；

c） 不同参与主体需根据业务角色确定数据存储的必要性，原则上，不应存储非本机构的 C3 类个人支付信息；

d） 个人支付信息的使用、加工应严格限制其使用目的。原则上，支付业务主体不应在支付业务以外的情形下使用个人支付信息；

e） 原则上，个人支付信息不应提供给非业务相关方，个人支付信息不允许公开。支付业务主体因商户在对账等活动的需要向其提供个人支付信息的，应对个人支付信息进行必要的脱敏处理，并要求商户做好个人支付信息的保护工作；

f） 个人支付信息的删除和销毁是防范支付信息泄露的重要手段。在个人支付信息不再需要使用时，可采取删除、销毁措施进行处理；

g） 涉及个人支付信息出境，应满足《个人信息保护法》、《数据出境安全评估办法》等法律法规的要求，符合规定的个人信息出境行为需要事前完成国家网信办组织的出境评估工作，跨境交易行为可能涉及个人金融信息出境，依规需要完成出境评估。

9 支付业务主体的安全保护范围

对于支付业务主体，个人支付信息保护需要覆盖以下范围：

a) 直接收集、存储、处理和传输个人支付信息的系统组件、人员和流程；
b) 可能不收集、存储、处理或传输个人支付信息的系统组件，但它们可以连接到存储、处理或传输个人支付信息的系统组件，且连接后对其访问行为没有有效的控制和审计的系统组件、人员和流程；
c) 可能影响个人支付信息处理环境安全的系统组件、人员和流程。

其中，系统组件包括但不限于：

a) 存储、处理或传输个人支付信息的系统（例如，支付终端、授权系统、清算系统、支付中间件系统、支付后台系统、购物车和店面系统、支付网关/开关系统、欺诈监控系统）；
b) 提供安全服务的系统（例如，验证服务器、访问控制服务器、安全信息和事件管理（SIEM）系统、物理安全系统（例如，标记访问或 CCTV）、多因素验证系统、反恶意软件系统）；
c) 实现网络分段的系统（例如，内部网络安全控制）；
d) 可能影响个人支付信息安全的系统（例如，名称解析，或电子商务（网络）重定向服务器）；
e) 虚拟化组件，例如虚拟机、虚拟交换机/路由器、虚拟设备、虚拟应用程序/桌面和虚拟机监视器；
f) 云基础设施和组件，包括外部和内部，并包括容器或图像的实例、虚拟私有云、基于云的身份和访问管理、驻留在内部或云中的个人支付信息处理环境、带有容器化应用程序的服务网格以及容器协调工具；
g) 网络组件，包括但不限于网络安全控制、交换机、路由器、VoIP 网络设备、无线接入点、网络设备和其他安全设备；
h) 服务器类型，包括但不限于 Web、应用程序、数据库、验证、邮件、代理、网络时间协议（NTP）和域名系统（DNS）；
i) 终端用户设备，例如计算机、笔记本、工作站、管理工作站、平板电脑和移动设备；
j) 打印机以及扫描、打印和传真的多功能设备；
k) 任何格式的存储账户数据（例如，纸质、数据文件、音频文件、图像和视频记录）；
l) 应用程序、软件和软件组件、无服务器应用程序，包括所有购买的、订阅的（例如，软件即服务）、定制软件，包括内部和外部（例如，互联网）应用程序；
m) 实施软件配置管理的工具、代码库和系统，或用于将对象部署到个人支付信息处理环境或可能影响个人支付信息处理环境的系统。

10 支付业务主体的基本要求

10.1 收单机构

收单机构应根据特约商户受理银行卡交易的真实场景，按照相关清算机构和发卡银行的业务规则和管理要求，正确选用交易类型，准确标识交易信息并完整发送，确保交易信息的完整性、真实性和可追溯性。

收单机构应切实履行特约商户检查责任，严格规范与外包服务机构业务合作，不应将收单业务交易处理、资金结算、风险监测、受理终端主密钥生成和管理、差错和争议处理工作交由外包服务机构办理；不应将外包服务机构拓展为特约商户并接收其发送的银行卡交易信息。

收单机构不应以任何形式存储银行卡磁道信息或芯片信息、卡片验证码、卡片有效期、个人标识码等信息，并应采取有效措施防止特约商户和外包服务机构存储此类信息。因特殊业务需要，收单机构确需存储的，应经持卡人本人及账户管理机构同意、确保存储的信息仅用于持卡人指定用途，并承担相应信息安全管理责任。

收单机构为境外特约商户提供银行卡收单服务的，应同时符合业务开办国家（地区）的监管要求。

10.2 账户机构

账户机构应依照中国人民银行有关客户信息保护的规定，制定有效的客户信息保护措施和风险控制机制，履行客户信息保护责任。

账户机构不应向其他机构或个人提供客户信息，法律法规另有规定，以及经客户本人逐项确认并授权的除外。

账户机构为客户开立支付账户的，应对客户实行实名制管理，登记并采取有效措施验证客户身份基本信息，按规定核对有效身份证件并留存有效身份证件复印件或者影印件，建立客户唯一识别编码，并在与客户业务关系存续期间采取持续的身份识别措施，确保有效核实客户身份及其真实意愿，不应开立匿名、假名支付账户。

账户机构应确保交易信息的真实性、完整性、可追溯性以及在支付全流程中的一致性，不应篡改或者隐匿交易信息。

10.3 清算机构

清算机构应遵守国家安全、国家网络安全相关法律法规，确保清算业务基础设施的安全、稳定和高效运行。清算业务基础设施应满足国家信息安全等级保护要求，使用经国家密码管理机构认可的商用密码产品，符合国家及行业相关金融标准，且其核心业务系统不应外包。

清算机构应对从清算服务中获取的身份信息、账户信息、交易信息以及其他相关信息等个人支付信息予以保密；除法律法规另有规定外，未经用户个人授权不应对外提供；清算机构处理用户个人授权的个人支付信息时，应通过业务规则及协议等有效措施，要求发卡机构或收单机构为所获得的个人支付信息保密。

10.4 其它相关机构

其它相关机构接受收单机构委托，为特约商户提供收单外包服务业务及相应服务的，应遵守《中华人民共和国个人信息保护法》等法律法规，遵循公开、透明原则，公开客户支付信息处理规则，明示处理的目的、方式和范围。基于客户同意处理个人支付信息的，该同意应由个人在充分知情的前提下自愿、明确做出。

其它相关机构因业务需要从支付指令或从支付指令以外获取的个人支付信息，应切实保护支付信息主体合法权益，保障信息安全，防范客户信息泄露、丢失、毁损或者被滥用，不应侵犯个人隐私和商业秘密。

其它相关机构应建立完善的客户信息安全管理制度和技术保障体系，从信息收集、 存储、传输、使用、 修改、删除、销毁等各环节制定相应的安全保护措施，采取有效技术手段防止支付信息泄露，聚合支付业务系统等相关系统应符合国家金融行业标准。

其它相关机构不应违规读取和存储客户银行卡密码、有效期、卡片验证码、磁道或芯片信息等个人支付信息。确需保存商户名称、交易金额、交易时间、客户 APP 标识、客户 IP 地址、交易介质等个人支付信息的，其它相关机构应对相关数据进行妥善保管，防止支付信息泄露。

11 支付业务主体的管理要求

11.1 组织架构

应建立个人支付信息保护的组织架构，并提供必要的资源，保障其独立履行职责。包括但不限于：

a） 成立由高级管理层构成的个人支付信息保护相关委员会，负责个人支付信息保护日常管理工作，委员会成员应至少涵盖本机构研发、测试、运维、风控、清算等与支付信息安全管理相关部门和具体负责人；

b） 个人支付信息保护相关委员会职责应包括但不限于：规划和建设支付信息安全管理机制、审批支付信息安全管理制度和流程、管理支付信息安全管理岗位职责和权限、推动支付信息安全管理制度落实、统筹支付信息安全事件应急处理；

c） 满足以下条件之一的组织，应设立专职的个人支付信息保护负责人和个人支付信息保护工作机构，负责个人支付信息安全工作：
- 主要业务涉及个人支付信息处理，且从业人员规模大于 200 人；
- 处理超过 100 万人的个人支付信息，或预计在 12 个月内处理超过 100 万人的个人支付信息；
- 处理超过 10 万人的 C2、C3 类个人支付信息的。

11.2 个人支付信息保护负责人

个人支付信息保护负责人应由具有相关管理工作经历和个人信息保护专业知识的人员担任，参与有关个人信息处理活动的重要决策，直接向组织主要负责人报告工作。

11.3 管理制度

a） 应将个人支付信息保护纳入到企业全面风险管理和内部控制流程中，建立适合机构条件的决策机制，制定有效的决策流程；
b） 制定个人支付信息保护风险管控机制，事前合规审查、事中监控跟踪、事后处置补救。在个人支付信息保护委员会的统一组织下，定期开展内部风险评估工作，定期面向金融消费者开展个人支付信息保护调研工作；
c） 制定个人支付信息保护相关信息披露的管理发布制度，并鼓励积极主动面向社会、监管机构发布信息披露报告；
d） 建立个人支付信息保护的教育培训机制，定期开展个人支付信息保护相关的教育培训活动，培训人员应覆盖个人支付信息保护全生命周期的参与人员。

11.4 岗位设置

各支付业务主体应根据自身业务特点合理设置人员岗位，确保各岗位根据“业务必须”和“最小化”原则，严格控制访问和使用支付信息，任何人都只能访问其开展业务所必需的支付信息，且只能够获得访问支付信息所必要的最小权限。防止未经授权擅自对支付信息进行查看、篡改和破坏。同时，应严格控制各岗位可能接触到的个人支付信息的数量。

应在个人支付信息保护的组织架构基础上，明确机构各层级内设部门与相关岗位个人支付信息保护职责与总体要求。

应明确在提供金融产品和服务的过程中知悉个人支付信息的岗位，并针对相关岗位明确其个人支付信息安全管理责任与保密责任，如不应未经授权的复制、存储、使用、共享、转让、披露个人支付信息。

12 支付业务主体的人员要求

12.1 人员录用

录用员工之前，需进行必要的背景调查，包括但不限于犯罪记录、简历核实、专业资格等，确保员工未从事或参与过危害持卡人支付信息安全或其他信息泄漏事件。

应与所有可访问支付信息的员工签署保密协议，或在劳动合同中设置保密条款。

应明确所有可访问支付信息岗位的支付信息安全责任、义务及相关惩罚措施等内容，并与所有可访问支付信息的员工签订支付信息安全责任承诺书。

12.2 人员培训

员工上岗前应及时安排其参加支付信息安全培训，培训内容包括但不限于支付信息安全管理制度、管理规定及操作流程、支付信息安全意识等相关内容，并保留原始培训记录。

应至少每年开展一次支付信息安全相关的培训或宣贯，提升员工的支付信息安全防护意识和技能，确保员工了解各自岗位职责、本岗位可访问支付信息的安全等级，以及违反安全规定可能导致的后果及惩罚措施，并保留相关记录至少 2 年。

12.3 人员转岗或离职

员工岗位调动或离职时，应立即变更、冻结或删除离岗员工对支付信息所有访问权限。
员工岗位调动或离职时，应立即取回相关身份证件、钥匙等物品以及机构提供的软硬件设备。
员工岗位调动或离职时，应办理严格的调离手续，并要求其履行保密义务。

12.4 违规人员管理

应对违反支付信息安全管理规定并造成C2、C3类支付信息泄漏事件的员工进行处罚，情节严重的应向相关监管部门报送违规员工个人信息并标明报送原因；涉嫌违法犯罪的，应及时报告公安机关。

13 支付业务主体的系统要求

支付业务主体应根据有关国家标准、行业标准、团体标准的相关要求，建立适当的安全能力，落实必要的管理和技术措施，防止个人支付信息的泄露、损毁、丢失、篡改，保证支付业务安全运行。

安全能力建设包括承载支付业务的信息系统、Web应用、客户端软件、支付终端等方面，其中信息系统、Web应用、客户端软件宜满足JR/T 0171—2020 6.2节中的相关要求，支付业务中使用的支付终端，根据其类型，宜满足T/PCAC 0003—2018和T/PCAC 0005—2019相关标准要求。承载个人支付信息的系统宜满足JR/T 0071—2020对应业务等级的要求。

14 不同业务场景的保护要求

支付业务主体宜根据不同场景设计个人支付信息的保护策略。建立个人支付信息保护基本要求，并在支付业务系统中正确、有效实现：

a) 用户支付场景的信息保护至少包含用户注册、用户信息变更、用户登录、支付、交易查询、用户注销等，参考14.1用户场景信息保护；
b) 运营场景信息保护主要包含运营人员进行信息查询、修改、删除等操作，参考14.2运营场景信息保护；
c) 运维场景信息保护主要关注数据库、日志等信息的保护，参考14.3运维场景信息保护。

14.1 用户场景信息保护

14.1.1用户注册

注册场景是用户在账户机构登记注册个人信息的过程，由账户机构完成信息收集动作。用户在银行业金融机构、非银行支付机构注册账户时，在满足监管部门关于账户实名制要求的基本前提下，宜参考下表进行信息保护。

参与主体 / 信息示例	用户	信息传递方向	账户服务方			
			收集	展示	处理（生成）	存储
姓名	人工录入，或通过OCR等技术手段识别	→	按照账户注册实名制要求收集信息。通过技术手段识别（如OCR识别身份证信息）时，需要确保识别结果的准确性	必要时展示，宜进行屏蔽展示	——	宜进行加密存储
身份证件	人工录入，或	→	按照账户注	必要时展示，	——	宜进行加密

信息	通过 OCR 等技术手段识别		册实名制要求收集信息	宜进行屏蔽展示		存储
电话号码	人工录入，或通过读取移动终端信息获取	→	通过 APP 或 SDK 等方式获得用户手机号信息时，需要取得用户同意	必要时展示，宜进行屏蔽展示	——	宜进行加密存储
联系地址	人工录入	→	用户录入	必要时展示，宜进行屏蔽展示	——	宜进行加密存储
用户口令	人工录入	→	用户录入	使用统一字符（如*或·）进行屏蔽展示；宜自定义输入框，不支持密码可见功能	——	加密存储，宜采取不可逆的加密算法
生物识别信息	通过设备采集	→	通过指纹识别器、摄像头等方式进行采集。需要取得用户同意。如果用户终端可以独立存储并进行验证，账户方不宜采集	一般不予以展示	——	加密存储，宜采取不可逆的加密算法。不宜存储原始生物识别信息
智能密码钥匙、OTP、证书	通过账户方获得	←	与获得的前述部分用户信息进行绑定	可显示对应的设备 ID 或证书编号、假名等，帮助用户识别	采用密码算法进行数据生成，确保不同的终端密钥均不相同	加密存储相关信息，宜采用挑战应答等机制
其他个人信息	人工录入，或通过移动终端采集。如采集用户注册时的终端信息、地理位置信息等	→	根据业务风控的需要，可以采集其他信息，但需要根据情况取得用户同意。通常情况下，此类信息采集失败不能作为禁止用户注册的理由	一般不予以展示	——	宜进行加密存储

14.1.2用户登录

登录场景是用户注册账户后通过身份认证获取后续服务的过程，由账户服务方完成信息收集和处理动作。用户在登录服务时，支付账户服务方通常不收集更多信息。用户提供错误的信息造成登录失败时，支付账户服务方宜及时清除不必要的信息。宜参考下表进行信息保护。

参与主体 / 信息示例	用户	信息传递方向	账户服务方			
			收集	展示	处理（生成）	存储
账号	人工录入（如采用手机号等也可能通过移动终端等进行读取）	→	用户录入的信息	通常全部展示，便于用户确认登录账号的正确性	通过密码算法处理，并与已经存储的账号进行比对	——
其他个人信息	一般通过移动终端采集。如采集用户登录时的终端信息、地理位置信息等	→	根据业务风控的需要，可以采集其他信息，但需要根据情况取得用户同意。通常情况下，此类信息采集失败不能作为禁止用户注册的理由	一般不予以展示	——	宜进行加密存储
用户口令	人工录入	→	用户录入	使用统一字符（如*或·）进行屏蔽展示；宜自定义输入框，不支持密码可见功能	——	——
生物识别信息	通过设备采集	→	通过指纹识别器、摄像头等方式进行采集。需要取得用户同意。如果用户终端可以独立存储并进行验证，账户方不宜采集	——	——	一般不存储新的生物识别信息，除非有信息更新的必要性
智能密码钥匙、OTP、证书	通过设备运算产生	→	——	——	采用对应的算法进行数据验证，确认用户是合法的持有者	——

14.1.3支付交易

不同的支付模式下，应对其处理的个人支付信息采取必要的保护措施。

14.1.3.1 网络支付

模式一：在线输入银行卡信息支付

参与主体 / 信息示例	用户	信息传递方向	商户支付页面（收单服务方）			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
银行卡号	输入	→	通过页面收集	加密	可存储	→	由收单机构转发	转加密	可存储	→	由转接清算机构转发	验证信息	加密存储
卡片验证码	输入	→	通过页面收集	加密	不存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储
有效期	输入	→	通过页面收集	加密	不建议存储	→	由收单机构转发	转加密	不建议存储	→	由转接清算机构转发	验证信息正确性	宜加密存储
PIN码	输入	→	通过页面收集	加密	不存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储

模式二：快捷支付（绑卡）

参与主体 / 信息示例	用户	信息传递方向	商户支付页面（收单服务方）			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
银行卡号	输入	→	通过页面收集	宜加密	可存储	→	由收单机构转发	转加密	可存储	→	由转接清算机构转发	验证信息	加密存储
卡片验证码	输入	→	通过页面收集	宜加密	不存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储

有效期	输入	→	通过页面收集	可加密	不建议存储	→	由收单机构转发	转加密	不建议存储	→	由转接清算机构转发	验证信息正确性	宜加密存储
身份信息	输入	→	通过页面收集	宜加密	不建议存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储
手机号	输入	→	通过页面收集	宜加密	不建议存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储

14.1.3.2 条码支付

主扫模式（商户展示收款码）1：静态码牌

参与主体 / 信息示例	用户	信息传递方向	商户支付页面（收单服务方）			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
条码（用户侧至账户侧）	1、访问收单方二维码支付地址	→	不涉及收单服务方和转接清算机构								调起密码键盘鉴权	——	加密存储
条码（收单侧至账户侧）	——	→	2、向账户侧请求openid/uid				不涉及清算机构			→	——	——	——
			3、关联id后组报文发送至清算机构		记录流水					→	4、由转接清算机构转发		

主扫模式（商户展示收款码）2：动态二维码预下单

参与主体 信息示例	用户	信息传递方向	商户支付页面（收单服务方）			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
条码（用户侧至账户侧）	4、用户扫描动态码	→	不涉及收单服务方和转接清算机构								——	——	——
条码（收单侧至账户侧）			1、商户向账户方申请支付订单		→					→			
			3、商户系统组装并生成二维码							←	2、账户方回传支付订单		

被扫模式（用户出示付款码）：

参与主体 信息示例	用户	信息传递方向	商户支付页面（收单服务方）			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
条码（用户侧）	申请获取或本地生成，默认不展示数字	←	不涉及收单服务方和转接清算机构								——	生成条码数据，参考JR T 0149—2016 中国金融移动支付 支	加密存储

					付标记化技术规范	

14.1.3.3银行卡收单

宜参考下表进行信息保护。

参与主体 / 信息示例	用户	信息传递方向	收单服务方			信息传递方向	转接清算机构			信息传递方向	账户服务方		
			收集	处理	存储		收集	处理	存储		收集	处理	存储
银行卡磁道信息或等效磁道信息	出示银行卡	→	通过读卡器读取	转加密	不存储	→	由收单机构转发	转加密	不存储	→	由转接清算机构转发	验证信息	加密存储
PIN码	通过密码键盘输入	→	通过密码键盘读取	转加密	不存储	→	由收单机构转发	转加密	宜进行加密存储	→	由转接清算机构转发	验证信息正确性	加密存储

14.1.4信息查询

非登录状态时，用户界面不宜显示完整的个人支付信息。可记住用户账号等信息便于用户快速登录。

登录状态下，仅显示查询范围内的必要信息。可使用屏蔽字符等方式降低泄露可能性，并采用点击显示全部的方式方便用户查看。为增加安全性，可根据需要在查询信息时再次进行身份验证。

14.1.5用户注销

用户注销时，应对用户进行再次身份核验。

宜使用用户注册时提交的身份信息进行验证，不再收集其他额外的信息。用户注销后，账户服务方宜及时对用户信息进行删除或匿名化处理。因法律法规和监管要求需要保留的信息除外。

14.2 运营场景信息保护

14.2.1信息查询

业务运营人员通过管理系统查询用户的个人支付信息时，管理系统需要记录操作员信息、操作原因等。如客服人员核对客户交易记录时，可能需要确认客户信息。

业务运营人员在批量访问个人支付信息时，宜限制访问批量数据；对于确需访问的，宜按照最小必要原则与业务目的一致性原则对其访问的信息数量进行控制，并做好日志记录，加强事前审批与事后审计。批量数据宜采取数据屏蔽的方式进行显示，避免录屏、拍摄等方式造成信息泄露。访问批量数据的数量、频次宜根据不同业务场景进行设置。

业务运营人员信息查询应遵循最小授权原则，在法律和相关安全策略允许的前提下，为满足工作需要，仅被授予其使用必要数据的最小权限。业务运营人员获取查询的数据具有保密责任，若其他人员有类似数据使用需求需另行申请，不应将获取数据进行公司内、外部共享、传播，若因对数据共享、传播等行为对公司造成不利影响甚至损失，将对其问责。不宜对C2、C3类数据直接进行明文的批量操作，例

如：导出、修改、拷贝等；对C2、C3数据设置每日查询次数上限，建议每天不超过100条；如因业务需要展示明文信息应对每次浏览明细C2、C3数据的行数进行限制，每次浏览的数据总量不应超过100行。

14.2.2信息修改

业务运营人员禁止以任何形式修改个人支付信息。运营人员登录系统后，应严格遵守法律法规要求及公司数据安全管理制度，把控数据使用用途和知晓人员范围，承担数据泄露、违规处理的相关责任。

14.2.3信息删除

业务运营人员禁止进行信息删除操作，管理平台不开启此项功能。相关操作均记录日志管理平台并定期进行业务安全审计工作，排查安全风险事件,确报数据安全。同一个用户不能被授予不相容的权限或角色（例如：系统管理员、业务操作员、审计员）。多人负责重要的权限、重要业务不能安排专人单独管理，须实行两人或多人相互制约的机制。

14.2.4数据分析

确保原始数据不出库，基于公司业务产生、收集、获得的原始数据均应保存在原授权主体数据环境内，原始数据原则上不应以任何形式直接对外输出。

如必须对原始数据进行加工，需以数据分析加工结果（如评分、验证、标签等）形式输出。数据使用应遵循严格的审批管理流程，未按规定进行审批、超出审批范围进行共享输出或变更输出形式等均属于违规行为，由直接责任人和主要责任人承担连带责任。

14.3 运维场景信息保护

序号	运维场景	保护要求
1	数据库管理	C2、C3类个人支付信息在数据库中应加密保存，降低通过数据库管理员运维造成数据泄密的风险。 数据库管理岗一般都有DBA权限，DBA权限有对数据库较高的包括增删改查等操作权限，数据库文件、数据表、数据等均存在被破坏或批量篡改的风险，因此该场景下主要考虑的技术保护措施： a） 数据库服务器配置最小网络访问权限，具备条件时可采取白名单网络访问控制策略； b） DBA配置最小账户访问权限，防止越权访问； c） 数据库管理操作中，启用操作审计日志功能，记录操作相关信息至少包括登录时间、登录账号，执行命令等； d） DBA账户登陆时采取双因素认证机制，在通过互联网远程登陆时，应使用VPN通道。
2	数据备份	在线备份一般为整库备份，通过备份工具，并采取全备+增量备份策略，备份介质通常为磁带、磁盘。 离线备份一般对数据进行查询操作，抽取出需要的表或字段，导出并保存在离线介质中，一般为磁盘或者移动存储介质。 相应的技术保护措施： a） 包含个人支付信息的备份介质，做好标签，注明是否含C3类个人支付信息； b） 备份时形成日志记录，或者备份操作记录台账； c） 存储介质存放于安全位置。
3	数据提取	数据提取方提出需求并由运维部门执行，然后按照预先商定的数据交付方式传递数据。运维部门执行时需要采取的技术保护要求： a） 设立数据提取岗，限制数据操作权限，仅保留数据查询操作权限； b） 数据提取记录台账。至少记录数据提取方、提取时间、数据操作人、提取包含哪些C2、C3类数据、数据交付方式、数据接收人、数据使用期限等。
4	数据介质销毁	数据介质销毁时： a） 介质回收利用时，应采取至少5次覆盖写入方式，确保磁盘数据不

		可恢复；介质不再循环利用时，采取物理消磁和物理损坏方式予以销毁； b） 销毁前有公司领导和执行部门负责人同意的审批手续； c） 销毁记录台账，至少记录销毁的时间、数据类型、介质及编号、销毁方式、执行人、确认人、明确的销毁记录存档方式、存档地点。
5	大数据平台数据抽取	通过数据抽取、数据转移工具等从各业务系统获取数据，需采取的技术保护要求： a） 基于大数据平台的定位，除非有必要，不建议在大数据平台长期存放 C2、C3 类个人支付信息； b） 涉及 C2、C3 类个人支付信息时，数据抽取范围发生变化或数据抽取脚本和程序变更时，要有相应的审批流程； c） 基于大数据平台进行数据分析时，不同的业务分析场景配置最小化数据访问权限，权限精细化到数据表或字段。
6	数据安全合规审计	设立专职合规审计岗位，负责审计对个人信息保护各场景中的合规要求落实情况。 留档书面审计报告，报告至少包括基本审计要素例如时间、审计人、审计范围、审计结果、整改建议等，侧重于对个人信息保护违规行为的描述。
7	日志信息处理	通常情况下，日志信息是对业务系统处理过程的记录。日志信息中包含个人支付信息，可能造成不必要的信息泄露风险。因而，典型做法是禁止在日志中留存任何 C3 类个人支付信息。 日志信息需要在特殊情况下辅助进行差错处理，如系统故障、处理错误等。因而，通常允许在日志中留存安全性要求较低的个人支付信息。对于日志中出现的个人支付信息，宜采取屏蔽的方式。

参考文献

[1] 中华人民共和国个人信息保护法，2021-8-20
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求
[4] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[5] JR/T 0098.8—2012 中国金融移动支付 检测规范 第8部分：个人信息保护
[6] JR/T 0001—2016 银行卡销售点（POS）终端技术规范
[7] JR/T 0149—2016 中国金融移动支付 支付标记化技术规范
[8] JR/T 0167—2018 云计算技术金融应用规范 安全技术要求
[9] JR/T 0092—2019 移动金融客户端应用软件安全管理规范
[10]JR/T 0071—2020 金融行业网络安全等级保护实施指引
[11]T/PCAC 0003—2018 银行卡销售点（POS）终端检测规范
[12]T/PCAC 0005—2019 条码支付受理终端检测规范
[13]银行卡业务管理办法（银发〔1999〕17号），1999-1-5
[14]《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》(银发〔2011〕17号),2011-1-21
[15]《中国人民银行关于银行业金融机构进一步做好客户个人金融信息保护工作的通知》(银发〔2012〕80号)，2012-3-27
[16]银行卡收单业务管理办法（中国人民银行公告〔2013〕第9号），2013-7-5
[17]非银行支付机构网络支付业务管理办法（中国人民银行公告〔2015〕第43号），2015-12-28
[18]银行卡清算机构管理办法(中国人民银行 中国银行业监督管理委员会令〔2016〕第2号)，2016-6-6
[19]《中国支付清算协会关于印发<收单外包服务机构自律规范（试行）>的通知》（中支协发〔2022〕12号），2022-1-27
[20]银联卡支付信息安全管理标准（银联风管委〔2018〕3号）,2018-7-5
[21]Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0, March 2022
[22]TC260-PG-20222A 《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》