2021

金融行业数据合规

法规与案例选编

Compilation of Data Compliance Laws and Cases for the Financial Industry

安证合规研究院
广东北源律师事务所 | 编

二〇二一年十一月

目录

编者说明

十八大以来，我国数据安全的顶层设计不断强化、治理格局日益稳定，初步构建了以《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》为主要框架的数据安全法律体系。

金融行业集中掌握了个人金融信息，涉及个人身份证明信息、财产信息、征信信息等敏感个人信息，属于国家重要数据。金融数据的安全影响国家安全、社会秩序、公共利益和金融市场的稳定。因此，金融行业的数据安全与合规的意义重大。

本汇编汇总了我国已公布或实施的多部金融行业数据合规有关的法律、行政法规、部门规章、规范性文件、国家标准、行业标准等文件，同时选编了近几年来金融业主管部门的监管典型执法案例，以帮助金融机构及有关企业或组织聚焦各类法规及监管执法的要求，有序开展数据合规和个人信息保护工作。

本汇编均选自 2021 年 10 月 28 日前公开发布的法规文件以及相关典型案例，若与将来正式公布实施的文件内容不一致，以正式文件为准。为尽可能全面收集金融行业有关法规及案例，节约阅读篇幅和时间，对部分法规或案例采取摘录或名录方式呈现。此外因标准指南内容版权限制，请读者自行登录国家标准全文系统等网站查阅相关标准全文。

本汇编同时在北源律所“个人信息保护合规平台”、“数据合规评估平台 PICA”（拟）上线，为实现线上多元化检索提供便利。本所将持续追踪该领域数据合规的最新立法和监管执法动态，后期根据新规、新政的出台，实时更新升级版本，欢迎批评指正和沟通交流。如对本汇编有任何疑问，请随时联系我们。

「关于北源」

广东北源律师事务所是一家专注于数据合规、个人信息保护等领域，具有国际视野的专业化律师事务所，以国内顶尖高校法学研究人才、国内领先的第三方计算机司法鉴定所和专业网络安全检测机构为依托组成，立足法律和技术的多元结合，兼具理论研究与实证经验。

「业绩和优势」

1. 2020 年 4 月开始，全面参与某国家监管部门发起的个人信息保护措施法律符合性评估试点工作，北源三位专家被聘为该试点工作的专家组专家，负责及完成三家头部企业的试点合规评估工作；

2. 发起并参与起草社会团体标准 T/CLAST001-2021《个人信息处理法律合规性评估指引》，该标准已于 2021 年 6 月 6 日正式发布实施；

3. 借助技术工具打造法律与技术结合的“个人信息保护合规评估平台”“数据合规评估平台 PICA”，以技术驱动合规评估流程实现全流程线上跟踪和电子数据固定，且实现评估结果可视化；

4. 案例入选《深圳经济特区四十年法治建设创新案例选编》；

5. 联合国内知名高校以及数字经济代表企业共同起草国内首创的《个人信息保护措施法律符合性评估指引》；

6. 入库多家世界 500 强法律服务提供商名单。

「案例展示」（部分）

1. 为世界五百强旗下保险领军企业的医疗险产品提供个人信息保护合规服务；

2. 为国内领先数字导航服务提供商的金融风控产品提供个人信息保护合规及咨询服务；

3. 为国内规模最大的移动应用数据平台服务商的 SDK 广告推送产品提供个人信息保护合规服务；

4. 为国内领先的第三方支付公司提供个人信息保护合规服务；

5. 为图像感知产品和解决方案提供商（中国人脸识别四大 A 级企业）提供数据合规咨询服务。

一、法律、法规、规章和其他规范性文件

（一）法律

中华人民共和国民法典

基本信息：	
【发布机关】全国人民代表大会	【时效性】现行有效
【发文字号】中华人民共和国主席令第 45 号	【效力级别】法律
【发布日期】2020.05.28	【实施日期】2021.01.01

中华人民共和国民法典（节选）

第一编 总则

第五章 民事权利

第一百一十条 自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。

法人、非法人组织享有名称权、名誉权和荣誉权。

第一百一十一条 自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

第四编 人格权

第一章 一般规定

第九百九十九条 为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等；使用不合理侵害民事主体人格权的，应当依法承担民事责任。

第一千条 行为人因侵害人格权承担消除影响、恢复名誉、赔礼道歉等民事责任的，应当与行为的具体方式和造成的影响范围相当。

行为人拒不承担前款规定的民事责任的，人民法院可以采取在报刊、网络等媒体上发布公告或者公布生效裁判文书等方式执行，产生的费用由行为人负担。

第五章 名誉权和荣誉权

第一千零三十条 民事主体与征信机构等信用信息处理者之间的关系，适用本编有关个人信息保护的规定和其他法律、行政法规的有关规定。

第六章 隐私权和个人信息保护

第一千零三十二条 自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

第一千零三十三条 除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：

（一）以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁；

（二）进入、拍摄、窥视他人的住宅、宾馆房间等私密空间；

（三）拍摄、窥视、窃听、公开他人的私密活动；

（四）拍摄、窥视他人身体的私密部位；

（五）处理他人的私密信息；

（六）以其他方式侵害他人的隐私权。

第一千零三十四条 自然人的个人信息受法律保护。

个人信息是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的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。

第一千零三十五条 处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：

（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；

（二）公开处理信息的规则；

（三）明示处理信息的目的、方式和范围；

（四）不违反法律、行政法规的规定和双方的约定。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

第一千零三十六条 处理个人信息，有下列情形之一的，行为人不承担民事责任：

（一）在该自然人或者其监护人同意的范围内合理实施的行为；

（二）合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明

确拒绝或者处理该信息侵害其重大利益的除外；

（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为。

第一千零三十七条 自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。

自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。

第一千零三十八条 信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。

信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、篡改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。

第一千零三十九条 国家机关、承担行政职能的法定机构及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或者向他人非法提供。

中华人民共和国刑法（2020 年修正）

基本信息：	
【发布机关】全国人民代表大会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第 66 号	【效力级别】法律
【发布日期】2020.12.26	【实施日期】2021.03.01

中华人民共和国刑法（2020 年修正）（节选）

第四章　侵犯公民人身权利、民主权利罪

第二百五十三条之一 【侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第六章　妨害社会管理秩序罪

第一节　扰乱公共秩序罪

第二百八十五条 【非法侵入计算机信息系统罪】违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

第二百八十六条 【破坏计算机信息系统罪】违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

第二百八十六条之一 【拒不履行信息网络安全管理义务罪】网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

（一）致使违法信息大量传播的；

（二）致使用户信息泄露，造成严重后果的；

（三）致使刑事案件证据灭失，情节严重的；

（四）有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

中华人民共和国网络安全法

基本信息：	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】主席令第53号	【效力级别】法律
【发布日期】2016.11.07	【实施日期】2017.06.01

中华人民共和国网络安全法【节选】

第一章 总则

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第三章 网络运行安全

第一节 一般规定

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二节　关键信息基础设施的运行安全

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第四章　网络信息安全

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或

者更正。

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第六章　法律责任

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不

改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章　附 则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

中华人民共和国数据安全法

基本信息：	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】中华人民共和国主席令第 84 号	【效力级别】法律
【发布日期】2021.06.10	【实施日期】2021.09.01

中华人民共和国数据安全法

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织

的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章 数据安全与发展

第十三条 国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条 国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条 国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条 国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条 国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个

人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告

知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有

关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自 2021 年 9 月 1 日起施行。

中华人民共和国个人信息保护法

基本信息：	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】中华人民共和国主席令第 91 号	【效力级别】法律
【发布日期】2021.08.20	【实施日期】2021.11.01

中华人民共和国个人信息保护法（2021）

第一章　总　则

第一条　为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条　自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条　在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

（一）以向境内自然人提供产品或者服务为目的；

（二）分析、评估境内自然人的行为；

（三）法律、行政法规规定的其他情形。

第四条　个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第五条　处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条　处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条　处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条　处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条　个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条　任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条　国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条　国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

第二章　个人信息处理规则

第一节　一般规定

第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：

（一）取得个人的同意；

（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；

（三）为履行法定职责或者法定义务所必需；

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条　基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自

愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条　基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条　个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十七条　个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

（一）个人信息处理者的名称或者姓名和联系方式；

（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）个人行使本法规定权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条　个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条　除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条　两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条　个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目

的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条　个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条　个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条　个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条　个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条　在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条　个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节　敏感个人信息的处理规则

第二十八条　敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、

医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条　处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条　个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

第三十一条　个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

第三十二条　法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节　国家机关处理个人信息的特别规定

第三十三条　国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条　国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条　国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条　国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条　法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章　个人信息跨境提供的规则

第三十八条　个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；

（四）法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条　个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。

第四十条　关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条　中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条　境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条　任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章　个人在个人信息处理活动中的权利

第四十四条　个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条　个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条　个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条　有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（三）个人撤回同意；

（四）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；

（五）法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条　个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条　自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条　个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章　个人信息处理者的义务

第五十一条　个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第五十二条　处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条　本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条　个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条　有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条　个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条　发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；

（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；

（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条　提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务：

（一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

（三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

（四）定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条　接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

第六章　履行个人信息保护职责的部门

第六十条　国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条　履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第六十二条　国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

（一）制定个人信息保护具体规则、标准；

（二）针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；

（三）支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；

（四）推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；

（五）完善个人信息保护投诉、举报工作机制。

第六十三条　履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

（一）询问有关当事人，调查与个人信息处理活动有关的情况；

（二）查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；

（三）实施现场检查，对涉嫌违法的个人信息处理活动进行调查；

（四）检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条　履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条　任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章　法律责任

第六十六条　违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条　国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条　处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

第七十条　个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条　违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章　附　　则

第七十二条　自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条　本法下列用语的含义：

（一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

（二）自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动。

（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十四条　本法自 2021 年 11 月 1 日起施行。

中华人民共和国中国人民银行法（2003 年修正）

基本信息：	
【发布机关】全国人大常委会	【时效性】现行有效
【发文字号】中华人民共和国主席令第 12 号	【效力级别】法律
【发布日期】2003.12.27	【实施日期】2004.02.01

中华人民共和国中国人民银行法（2003 年修正）（节选）

第五章 金融监督管理

第三十一条 中国人民银行依法监测金融市场的运行情况，对金融市场实施宏观调控，促进其协调发展。

第三十二条 中国人民银行有权对金融机构以及其他单位和个人的下列行为进行检查监督：

（一）执行有关存款准备金管理规定的行为；

（二）与中国人民银行特种贷款有关的行为；

（三）执行有关人民币管理规定的行为；

（四）执行有关银行间同业拆借市场、银行间债券市场管理规定的行为；

（五）执行有关外汇管理规定的行为；

（六）执行有关黄金管理规定的行为；

（七）代理中国人民银行经理国库的行为；

（八）执行有关清算管理规定的行为；

（九）执行有关反洗钱规定的行为。

前款所称中国人民银行特种贷款，是指国务院决定的由中国人民银行向金融机构发放的用于特定目的的贷款。

第三十三条 中国人民银行根据执行货币政策和维护金融稳定的需要，可以建议国务院银行业监督管理机构对银行业金融机构进行检查监督。国务院银行业监督管理机构应当自收到建议之日起三十日内予以回复。

第三十四条 当银行业金融机构出现支付困难，可能引发金融风险时，为了维护金融稳定，中国人民银行经国务院批准，有权对银行业金融机构进行检查监督。

第三十五条 中国人民银行根据履行职责的需要，有权要求银行业金融机构报送必要的资产负债表、利润表以及其他财务会计、统计报表和资料。

中国人民银行应当和国务院银行业监督管理机构、国务院其他金融监督管理机构建立监督管理信息共享机制。

第三十六条 中国人民银行负责统一编制全国金融统计数据、报表，并按照国家有关规定予以公布。

第三十七条 中国人民银行应当建立、健全本系统的稽核、检查制度，加强内部的监督管理。

中华人民共和国银行业监督管理法（2006 年修正）

基本信息：	
【发布机关】全国人民代表大会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第 58 号	【效力级别】法律
【发布日期】2006.10.31	【实施日期】2007.01.01

中华人民共和国银行业监督管理法（2006 年修正）

第一章 总 则

第一条 为了加强对银行业的监督管理，规范监督管理行为，防范和化解银行业风险，保护存款人和其他客户的合法权益，促进银行业健康发展，制定本法。

第二条 国务院银行业监督管理机构负责对全国银行业金融机构及其业务活动监督管理的工作。

本法所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、城市信用合

作社、农村信用合作社等吸收公众存款的金融机构以及政策性银行。

对在中华人民共和国境内设立的金融资产管理公司、信托投资公司、财务公司、金融租赁公司以及经国务院银行业监督管理机构批准设立的其他金融机构的监督管理，适用本法对银行业金融机构监督管理的规定。

国务院银行业监督管理机构依照本法有关规定，对经其批准在境外设立的金融机构以及前二款金融机构在境外的业务活动实施监督管理。

第三条　银行业监督管理的目标是促进银行业的合法、稳健运行，维护公众对银行业的信心。

银行业监督管理应当保护银行业公平竞争，提高银行业竞争能力。

第四条　银行业监督管理机构对银行业实施监督管理，应当遵循依法、公开、公正和效率的原则。

第五条　银行业监督管理机构及其从事监督管理工作的人员依法履行监督管理职责，受法律保护。地方政府、各级政府部门、社会团体和个人不得干涉。

第六条　国务院银行业监督管理机构应当和中国人民银行、国务院其他金融监督管理机构建立监督管理信息共享机制。

第七条　国务院银行业监督管理机构可以和其他国家或者地区的银行业监督管理机构建立监督管理合作机制，实施跨境监督管理。

第二章　监督管理机构

第八条　国务院银行业监督管理机构根据履行职责的需要设立派出机构。国务院银行业监督管理机构对派出机构实行统一领导和管理。

国务院银行业监督管理机构的派出机构在国务院银行业监督管理机构的授权范围内，履行监督管理职责。

第九条　银行业监督管理机构从事监督管理工作的人员，应当具备与其任职相适应的专业知识和业务工作经验。

第十条　银行业监督管理机构工作人员，应当忠于职守，依法办事，公正廉洁，不得利用职务便利牟取不正当的利益，不得在金融机构等企业中兼任职务。

第十一条　银行业监督管理机构工作人员，应当依法保守国家秘密，并有责任为其监督管理的银行业金融机构及当事人保守秘密。

国务院银行业监督管理机构同其他国家或者地区的银行业监督管理机构交流监督管理信息，应当就信息保密作出安排。

第十二条　国务院银行业监督管理机构应当公开监督管理程序，建立监督管理责任制度和内部监督制度。

第十三条　银行业监督管理机构在处置银行业金融机构风险、查处有关金融违法行为等监督管理活动中，地方政府、各级有关部门应当予以配合和协助。

第十四条　国务院审计、监察等机关，应当依照法律规定对国务院银行业监督管理机构的活动进行监督。

第三章　监督管理职责

第十五条　国务院银行业监督管理机构依照法律、行政法规制定并发布对银行业金融机构及其业务活动监督管理的规章、规则。

第十六条　国务院银行业监督管理机构依照法律、行政法规规定的条件和程序，审查批准银行业金融机构的设立、变更、终止以及业务范围。

第十七条　申请设立银行业金融机构，或者银行业金融机构变更持有资本总额或者股份总额达到规定比例以上的股东的，国务院银行业监督管理机构应当对股东的资金来源、财务状况、资本补充能力和诚信状况进行审查。

第十八条　银行业金融机构业务范围内的业务品种，应当按照规定经国务院银行业监督管理机构审查批准或者备案。需要审查批准或者备案的业务品种，由国务院银行业监督管理机构依照法律、行政法规作出规定并公布。

第十九条　未经国务院银行业监督管理机构批准，任何单位或者个人不得设立银行业金融机构或者从事银行业金融机构的业务活动。

第二十条　国务院银行业监督管理机构对银行业金融机构的董事和高级管理人员实行任职资格管理。具体办法由国务院银行业监督管理机构制定。

第二十一条　银行业金融机构的审慎经营规则，由法律、行政法规规定，也可以由国务院银行业监督管理机构依照法律、行政法规制定。

前款规定的审慎经营规则，包括风险管理、内部控制、资本充足率、资产质量、损失准备金、风险集中、关联交易、资产流动性等内容。

银行业金融机构应当严格遵守审慎经营规则。

第二十二条　国务院银行业监督管理机构应当在规定的期限，对下列申请事项作出批准或者不批准的书面决定；决定不批准的，应当说明理由：

（一）银行业金融机构的设立，自收到申请文件之日起六个月内；

（二）银行业金融机构的变更、终止，以及业务范围和增加业务范围内的业务品种，

自收到申请文件之日起三个月内；

（三）审查董事和高级管理人员的任职资格，自收到申请文件之日起三十日内。

第二十三条　银行业监督管理机构应当对银行业金融机构的业务活动及其风险状况进行非现场监管，建立银行业金融机构监督管理信息系统，分析、评价银行业金融机构的风险状况。

第二十四条　银行业监督管理机构应当对银行业金融机构的业务活动及其风险状况进行现场检查。

国务院银行业监督管理机构应当制定现场检查程序，规范现场检查行为。

第二十五条　国务院银行业监督管理机构应当对银行业金融机构实行并表监督管理。

第二十六条　国务院银行业监督管理机构对中国人民银行提出的检查银行业金融机构的建议，应当自收到建议之日起三十日内予以回复。

第二十七条　国务院银行业监督管理机构应当建立银行业金融机构监督管理评级体系和风险预警机制，根据银行业金融机构的评级情况和风险状况，确定对其现场检查的频率、范围和需要采取的其他措施。

第二十八条　国务院银行业监督管理机构应当建立银行业突发事件的发现、报告岗位责任制度。

银行业监督管理机构发现可能引发系统性银行业风险、严重影响社会稳定的突发事件的，应当立即向国务院银行业监督管理机构负责人报告；国务院银行业监督管理机构负责人认为需要向国务院报告的，应当立即向国务院报告，并告知中国人民银行、国务院财政部门等有关部门。

第二十九条　国务院银行业监督管理机构应当会同中国人民银行、国务院财政部门等有关部门建立银行业突发事件处置制度，制定银行业突发事件处置预案，明确处置机构和人员及其职责、处置措施和处置程序，及时、有效地处置银行业突发事件。

第三十条　国务院银行业监督管理机构负责统一编制全国银行业金融机构的统计数据、报表，并按照国家有关规定予以公布。

第三十一条　国务院银行业监督管理机构对银行业自律组织的活动进行指导和监督。

银行业自律组织的章程应当报国务院银行业监督管理机构备案。

第三十二条　国务院银行业监督管理机构可以开展与银行业监督管理有关的国际交流、合作活动。

第四章　监督管理措施

第三十三条　银行业监督管理机构根据履行职责的需要，有权要求银行业金融机构按照规定报送资产负债表、利润表和其他财务会计、统计报表、经营管理资料以及注册会计师出具的审计报告。

第三十四条　银行业监督管理机构根据审慎监管的要求，可以采取下列措施进行现场检查：

（一）进入银行业金融机构进行检查；

（二）询问银行业金融机构的工作人员，要求其对有关检查事项作出说明；

（三）查阅、复制银行业金融机构与检查事项有关的文件、资料，对可能被转移、隐匿或者毁损的文件、资料予以封存；

（四）检查银行业金融机构运用电子计算机管理业务数据的系统。

进行现场检查，应当经银行业监督管理机构负责人批准。现场检查时，检查人员不得少于二人，并应当出示合法证件和检查通知书；检查人员少于二人或者未出示合法证件和检查通知书的，银行业金融机构有权拒绝检查。

第三十五条　银行业监督管理机构根据履行职责的需要，可以与银行业金融机构董事、高级管理人员进行监督管理谈话，要求银行业金融机构董事、高级管理人员就银行业金融机构的业务活动和风险管理的重大事项作出说明。

第三十六条　银行业监督管理机构应当责令银行业金融机构按照规定，如实向社会公众披露财务会计报告、风险管理状况、董事和高级管理人员变更以及其他重大事项等信息。

第三十七条　银行业金融机构违反审慎经营规则的，国务院银行业监督管理机构或者其省一级派出机构应当责令限期改正；逾期未改正的，或者其行为严重危及该银行业金融机构的稳健运行、损害存款人和其他客户合法权益的，经国务院银行业监督管理机构或者其省一级派出机构负责人批准，可以区别情形，采取下列措施：

（一）责令暂停部分业务、停止批准开办新业务；

（二）限制分配红利和其他收入；

（三）限制资产转让；

（四）责令控股股东转让股权或者限制有关股东的权利；

（五）责令调整董事、高级管理人员或者限制其权利；

（六）停止批准增设分支机构。

银行业金融机构整改后，应当向国务院银行业监督管理机构或者其省一级派出机构提交报告。国务院银行业监督管理机构或者其省一级派出机构经验收，符合有关审慎经营规

则的，应当自验收完毕之日起三日内解除对其采取的前款规定的有关措施。

第三十八条　银行业金融机构已经或者可能发生信用危机，严重影响存款人和其他客户合法权益的，国务院银行业监督管理机构可以依法对该银行业金融机构实行接管或者促成机构重组，接管和机构重组依照有关法律和国务院的规定执行。

第三十九条　银行业金融机构有违法经营、经营管理不善等情形，不予撤销将严重危害金融秩序、损害公众利益的，国务院银行业监督管理机构有权予以撤销。

第四十条　银行业金融机构被接管、重组或者被撤销的，国务院银行业监督管理机构有权要求该银行业金融机构的董事、高级管理人员和其他工作人员，按照国务院银行业监督管理机构的要求履行职责。

在接管、机构重组或者撤销清算期间，经国务院银行业监督管理机构负责人批准，对直接负责的董事、高级管理人员和其他直接责任人员，可以采取下列措施：

（一）直接负责的董事、高级管理人员和其他直接责任人员出境将对国家利益造成重大损失的，通知出境管理机关依法阻止其出境；

（二）申请司法机关禁止其转移、转让财产或者对其财产设定其他权利。

第四十一条　经国务院银行业监督管理机构或者其省一级派出机构负责人批准，银行业监督管理机构有权查询涉嫌金融违法的银行业金融机构及其工作人员以及关联行为人的账户；对涉嫌转移或者隐匿违法资金的，经银行业监督管理机构负责人批准，可以申请司法机关予以冻结。

第四十二条　银行业监督管理机构依法对银行业金融机构进行检查时，经设区的市一级以上银行业监督管理机构负责人批准，可以对与涉嫌违法事项有关的单位和个人采取下列措施：

（一）询问有关单位或者个人，要求其对有关情况作出说明；

（二）查阅、复制有关财务会计、财产权登记等文件、资料；

（三）对可能被转移、隐匿、毁损或者伪造的文件、资料，予以先行登记保存。

银行业监督管理机构采取前款规定措施，调查人员不得少于二人，并应当出示合法证件和调查通知书；调查人员少于二人或者未出示合法证件和调查通知书的，有关单位或者个人有权拒绝。对依法采取的措施，有关单位和个人应当配合，如实说明有关情况并提供有关文件、资料，不得拒绝、阻碍和隐瞒。

第五章　法律责任

第四十三条　银行业监督管理机构从事监督管理工作的人员有下列情形之一的，依法

给予行政处分；构成犯罪的，依法追究刑事责任：

（一）违反规定审查批准银行业金融机构的设立、变更、终止，以及业务范围和业务范围内的业务品种的；

（二）违反规定对银行业金融机构进行现场检查的；

（三）未依照本法第二十八条规定报告突发事件的；

（四）违反规定查询账户或者申请冻结资金的；

（五）违反规定对银行业金融机构采取措施或者处罚的；

（六）违反本法第四十二条规定对有关单位或者个人进行调查的；

（七）滥用职权、玩忽职守的其他行为。

银行业监督管理机构从事监督管理工作的人员贪污受贿，泄露国家秘密、商业秘密和个人隐私，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，依法给予行政处分。

第四十四条　擅自设立银行业金融机构或者非法从事银行业金融机构的业务活动的，由国务院银行业监督管理机构予以取缔；构成犯罪的，依法追究刑事责任；尚不构成犯罪的，由国务院银行业监督管理机构没收违法所得，违法所得五十万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五十万元的，处五十万元以上二百万元以下罚款。

第四十五条　银行业金融机构有下列情形之一，由国务院银行业监督管理机构责令改正，有违法所得的，没收违法所得，违法所得五十万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五十万元的，处五十万元以上二百万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经批准设立分支机构的；

（二）未经批准变更、终止的；

（三）违反规定从事未经批准或者未备案的业务活动的；

（四）违反规定提高或者降低存款利率、贷款利率的。

第四十六条　银行业金融机构有下列情形之一，由国务院银行业监督管理机构责令改正，并处二十万元以上五十万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经任职资格审查任命董事、高级管理人员的；

（二）拒绝或者阻碍非现场监管或者现场检查的；

（三）提供虚假的或者隐瞒重要事实的报表、报告等文件、资料的；

（四）未按照规定进行信息披露的；

（五）严重违反审慎经营规则的；

（六）拒绝执行本法第三十七条规定的措施的。

第四十七条　银行业金融机构不按照规定提供报表、报告等文件、资料的，由银行业监督管理机构责令改正，逾期不改正的，处十万元以上三十万元以下罚款。

第四十八条　银行业金融机构违反法律、行政法规以及国家有关银行业监督管理规定的，银行业监督管理机构除依照本法第四十四条至第四十七条规定处罚外，还可以区别不同情形，采取下列措施：

（一）责令银行业金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分；

（二）银行业金融机构的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员给予警告，处五万元以上五十万元以下罚款；

（三）取消直接负责的董事、高级管理人员一定期限直至终身的任职资格，禁止直接负责的董事、高级管理人员和其他直接责任人员一定期限直至终身从事银行业工作。

第四十九条　阻碍银行业监督管理机构工作人员依法执行检查、调查职务的，由公安机关依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第六章　附　则

第五十条　对在中华人民共和国境内设立的政策性银行、金融资产管理公司的监督管理，法律、行政法规另有规定的，依照其规定。

第五十一条　对在中华人民共和国境内设立的外资银行业金融机构、中外合资银行业金融机构、外国银行业金融机构的分支机构的监督管理，法律、行政法规另有规定的，依照其规定。

第五十二条　本法自 2004 年 2 月 1 日起施行。

中华人民共和国反洗钱法

基本信息：	
【发布机关】全国人民代表大会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第 56 号	【效力级别】法律
【发布日期】2006.10.31	【实施日期】2007.7.1

中华人民共和国反洗钱法（节选）

第一章　总　则

第五条　对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供。

反洗钱行政主管部门和其他依法负有反洗钱监督管理职责的部门、机构履行反洗钱职责获得的客户身份资料和交易信息，只能用于反洗钱行政调查。

司法机关依照本法获得的客户身份资料和交易信息，只能用于反洗钱刑事诉讼。

第二章　反洗钱监督管理

第十一条　国务院反洗钱行政主管部门为履行反洗钱资金监测职责，可以从国务院有关部门、机构获取所必需的信息，国务院有关部门、机构应当提供。

国务院反洗钱行政主管部门应当向国务院有关部门、机构定期通报反洗钱工作情况。

第三章　金融机构反洗钱义务

第十七条　金融机构通过第三方识别客户身份的，应当确保第三方已经采取符合本法要求的客户身份识别措施；第三方未采取符合本法要求的客户身份识别措施的，由该金融机构承担未履行客户身份识别义务的责任。

第十九条　金融机构应当按照规定建立客户身份资料和交易记录保存制度。

在业务关系存续期间，客户身份资料发生变更的，应当及时更新客户身份资料。

客户身份资料在业务关系结束后、客户交易信息在交易结束后，应当至少保存五年。

金融机构破产和解散时，应当将客户身份资料和客户交易信息移交国务院有关部门指定的机构。

第五章　反洗钱国际合作

第二十八条　国务院反洗钱行政主管部门根据国务院授权，代表中国政府与外国政府和有关国际组织开展反洗钱合作，依法与境外反洗钱机构交换与反洗钱有关的信息和资料。

中华人民共和国消费者权益保护法（2013 年修正）

基本信息：	
【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第 7 号	【效力级别】法律
【发布日期】2013.10.25	【实施日期】2014.03.15

中华人民共和国消费者权益保护法（2013 年修正）（节选）

第十四条 消费者在购买、使用商品和接受服务时，享有人格尊严、民族风俗习惯得到尊重的权利，享有个人信息依法得到保护的权利。

第二十条 经营者向消费者提供有关商品或者服务的质量、性能、用途、有效期限等信息，应当真实、全面，不得作虚假或者引人误解的宣传。

经营者对消费者就其提供的商品或者服务的质量和使用方法等问题提出的询问，应当作出真实、明确的答复。

经营者提供商品或者服务应当明码标价。

第二十八条 采用网络、电视、电话、邮购等方式提供商品或者服务的经营者，以及提供证券、保险、银行等金融服务的经营者，应当向消费者提供经营地址、联系方式、商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险警示、售后服务、民事责任等信息。

第二十九条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

经营者及其工作人员对收集的消费者个人信息必须严格保密，不得泄露、出售或者非法向他人提供。经营者应当采取技术措施和其他必要措施，确保信息安全，防止消费者个人信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。

经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性信息。

第五十条 经营者侵害消费者的人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的，应当停止侵害、恢复名誉、消除影响、赔礼道歉，并赔偿损失。

第五十六条 经营者有下列情形之一，除承担相应的民事责任外，其他有关法律、法规

对处罚机关和处罚方式有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由工商行政管理部门或者其他有关行政部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得一倍以上十倍以下的罚款，没有违法所得的，处以五十万元以下的罚款；情节严重的，责令停业整顿、吊销营业执照：

（一）提供的商品或者服务不符合保障人身、财产安全要求的；

（二）在商品中掺杂、掺假，以假充真，以次充好，或者以不合格商品冒充合格商品的；

（三）生产国家明令淘汰的商品或者销售失效、变质的商品的；

（四）伪造商品的产地，伪造或者冒用他人的厂名、厂址，篡改生产日期，伪造或者冒用认证标志等质量标志的；

（五）销售的商品应当检验、检疫而未检验、检疫或者伪造检验、检疫结果的；

（六）对商品或者服务作虚假或者引人误解的宣传的；

（七）拒绝或者拖延有关行政部门责令对缺陷商品或者服务采取停止销售、警示、召回、无害化处理、销毁、停止生产或者服务等措施的；

（八）对消费者提出的修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失的要求，故意拖延或者无理拒绝的；

（九）侵害消费者人格尊严、侵犯消费者人身自由或者侵害消费者个人信息依法得到保护的权利的；

（十）法律、法规规定的对损害消费者权益应当予以处罚的其他情形。

经营者有前款规定情形的，除依照法律、法规规定予以处罚外，处罚机关应当记入信用档案，向社会公布。

中华人民共和国商业银行法（2015 年修正）

基本信息：

【发布机关】全国人大常委会	【时效性】 现行有效
【发文字号】中华人民共和国主席令第 34 号	【效力级别】法律
【发布日期】2015.08.29	【实施日期】2015.10.01

中华人民共和国商业银行法（2015 年修正）（节选）

第六章 监督管理

第五十九条 商业银行应当按照有关规定，制定本行的业务规则，建立、健全本行的风险管理和内部控制制度。

第六十条 商业银行应当建立、健全本行对存款、贷款、结算、呆账等各项情况的稽核、检查制度。

商业银行对分支机构应当进行经常性的稽核和检查监督。

第六十一条 商业银行应当按照规定向国务院银行业监督管理机构、中国人民银行报送资产负债表、利润表以及其他财务会计、统计报表和资料。

第六十二条 国务院银行业监督管理机构有权依照本法第三章、第四章、第五章的规定，随时对商业银行的存款、贷款、结算、呆账等情况进行检查监督。检查监督时，检查监督人员应当出示合法的证件。商业银行应当按照国务院银行业监督管理机构的要求，提供财务会计资料、业务合同和有关经营管理方面的其他信息。

中国人民银行有权依照《中华人民共和国中国人民银行法》第三十二条、第三十四条的规定对商业银行进行检查监督。

第六十三条 商业银行应当依法接受审计机关的审计监督。

第七章 接管和终止

第六十四条 商业银行已经或者可能发生信用危机，严重影响存款人的利益时，国务院银行业监督管理机构可以对该银行实行接管。

接管的目的是对被接管的商业银行采取必要措施，以保护存款人的利益，恢复商业银行的正常经营能力。被接管的商业银行的债权债务关系不因接管而变化。

第六十五条 接管由国务院银行业监督管理机构决定，并组织实施。国务院银行业监督管理机构的接管决定应当载明下列内容：

（一）被接管的商业银行名称；

（二）接管理由；

（三）接管组织；

（四）接管期限。

接管决定由国务院银行业监督管理机构予以公告。

第六十六条 接管自接管决定实施之日起开始。

自接管开始之日起，由接管组织行使商业银行的经营管理权力。

第六十七条 接管期限届满，国务院银行业监督管理机构可以决定延期，但接管期限最

长不得超过二年。

第六十八条 有下列情形之一的，接管终止：

（一）接管决定规定的期限届满或者国务院银行业监督管理机构决定的接管延期届满；

（二）接管期限届满前，该商业银行已恢复正常经营能力；

（三）接管期限届满前，该商业银行被合并或者被依法宣告破产。

第六十九条 商业银行因分立、合并或者出现公司章程规定的解散事由需要解散的，应当向国务院银行业监督管理机构提出申请，并附解散的理由和支付存款的本金和利息等债务清偿计划。经国务院银行业监督管理机构批准后解散。

商业银行解散的，应当依法成立清算组，进行清算，按照清偿计划及时偿还存款本金和利息等债务。国务院银行业监督管理机构监督清算过程。

第七十条 商业银行因吊销经营许可证被撤销的，国务院银行业监督管理机构应当依法及时组织成立清算组，进行清算，按照清偿计划及时偿还存款本金和利息等债务。

第七十一条 商业银行不能支付到期债务，经国务院银行业监督管理机构同意，由人民法院依法宣告其破产。商业银行被宣告破产的，由人民法院组织国务院银行业监督管理机构等有关部门和有关人员成立清算组，进行清算。

商业银行破产清算时，在支付清算费用、所欠职工工资和劳动保险费用后，应当优先支付个人储蓄存款的本金和利息。

第七十二条 商业银行因解散、被撤销和被宣告破产而终止。

第八章 法律责任

第七十三条 商业银行有下列情形之一，对存款人或者其他客户造成财产损害的，应当承担支付迟延履行的利息以及其他民事责任：

（一）无故拖延、拒绝支付存款本金和利息的；

（二）违反票据承兑等结算业务规定，不予兑现，不予收付入账，压单、压票或者违反规定退票的；

（三）非法查询、冻结、扣划个人储蓄存款或者单位存款的；

（四）违反本法规定对存款人或者其他客户造成损害的其他行为。

有前款规定情形的，由国务院银行业监督管理机构责令改正，有违法所得的，没收违法所得，违法所得五万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五万元的，处五万元以上五十万元以下罚款。

第七十四条 商业银行有下列情形之一，由国务院银行业监督管理机构责令改正，有违法所得的，没收违法所得，违法所得五十万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五十万元的，处五十万元以上二百万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经批准设立分支机构的；

（二）未经批准分立、合并或者违反规定对变更事项不报批的；

（三）违反规定提高或者降低利率以及采用其他不正当手段，吸收存款，发放贷款的；

（四）出租、出借经营许可证的；

（五）未经批准买卖、代理买卖外汇的；

（六）未经批准买卖政府债券或者发行、买卖金融债券的；

（七）违反国家规定从事信托投资和证券经营业务、向非自用不动产投资或者向非银行金融机构和企业投资的；

（八）向关系人发放信用贷款或者发放担保贷款的条件优于其他借款人同类贷款的条件的。

第七十五条 商业银行有下列情形之一，由国务院银行业监督管理机构责令改正，并处二十万元以上五十万元以下罚款；情节特别严重或者逾期不改正的，可以责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）拒绝或者阻碍国务院银行业监督管理机构检查监督的；

（二）提供虚假的或者隐瞒重要事实的财务会计报告、报表和统计报表的；

（三）未遵守资本充足率、资产流动性比例、同一借款人贷款比例和国务院银行业监督管理机构有关资产负债比例管理的其他规定的。

第七十六条 商业银行有下列情形之一，由中国人民银行责令改正，有违法所得的，没收违法所得，违法所得五十万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五十万元的，处五十万元以上二百万元以下罚款；情节特别严重或者逾期不改正的，中国人民银行可以建议国务院银行业监督管理机构责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）未经批准办理结汇、售汇的；

（二）未经批准在银行间债券市场发行、买卖金融债券或者到境外借款的；

（三）违反规定同业拆借的。

第七十七条 商业银行有下列情形之一，由中国人民银行责令改正，并处二十万元以上五十万元以下罚款；情节特别严重或者逾期不改正的，中国人民银行可以建议国务院银行业监督管理机构责令停业整顿或者吊销其经营许可证；构成犯罪的，依法追究刑事责任：

（一）拒绝或者阻碍中国人民银行检查监督的；

（二）提供虚假的或者隐瞒重要事实的财务会计报告、报表和统计报表的；

（三）未按照中国人民银行规定的比例交存存款准备金的。

第七十八条 商业银行有本法第七十三条至第七十七条规定情形的，对直接负责的董事、高级管理人员和其他直接责任人员，应当给予纪律处分；构成犯罪的，依法追究刑事责任。

第七十九条 有下列情形之一，由国务院银行业监督管理机构责令改正，有违法所得的，没收违法所得，违法所得五万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五万元的，处五万元以上五十万元以下罚款：

（一）未经批准在名称中使用“银行”字样的；

（二）未经批准购买商业银行股份总额百分之五以上的；

（三）将单位的资金以个人名义开立账户存储的。

第八十条 商业银行不按照规定向国务院银行业监督管理机构报送有关文件、资料的，由国务院银行业监督管理机构责令改正，逾期不改正的，处十万元以上三十万元以下罚款。

商业银行不按照规定向中国人民银行报送有关文件、资料的，由中国人民银行责令改正，逾期不改正的，处十万元以上三十万元以下罚款。

第八十一条未经国务院银行业监督管理机构批准，擅自设立商业银行，或者非法吸收公众存款、变相吸收公众存款，构成犯罪的，依法追究刑事责任；并由国务院银行业监督管理机构予以取缔。

伪造、变造、转让商业银行经营许可证，构成犯罪的，依法追究刑事责任。

第八十二条 借款人采取欺诈手段骗取贷款，构成犯罪的，依法追究刑事责任。

第八十三条 有本法第八十一条、第八十二条规定的行为，尚不构成犯罪的，由国务院银行业监督管理机构没收违法所得，违法所得五十万元以上的，并处违法所得一倍以上五倍以下罚款；没有违法所得或者违法所得不足五十万元的，处五十万元以上二百万元以下罚款。

第八十四条 商业银行工作人员利用职务上的便利，索取、收受贿赂或者违反国家规定收受各种名义的回扣、手续费，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，应当给予纪律处分。

有前款行为，发放贷款或者提供担保造成损失的，应当承担全部或者部分赔偿责任。

第八十五条 商业银行工作人员利用职务上的便利，贪污、挪用、侵占本行或者客户资金，构成犯罪的，依法追究刑事责任；尚不构成犯罪的，应当给予纪律处分。

第八十六条 商业银行工作人员违反本法规定玩忽职守造成损失的，应当给予纪律处分；构成犯罪的，依法追究刑事责任。

违反规定徇私向亲属、朋友发放贷款或者提供担保造成损失的，应当承担全部或者部分赔偿责任。

第八十七条 商业银行工作人员泄露在任职期间知悉的国家秘密、商业秘密的，应当给予纪律处分；构成犯罪的，依法追究刑事责任。

第八十八条 单位或者个人强令商业银行发放贷款或者提供担保的，应当对直接负责的主管人员和其他直接责任人员或者个人给予纪律处分；造成损失的，应当承担全部或者部分赔偿责任。

商业银行的工作人员对单位或者个人强令其发放贷款或者提供担保未予拒绝的，应当给予纪律处分；造成损失的，应当承担相应的赔偿责任。

第八十九条 商业银行违反本法规定的，国务院银行业监督管理机构可以区别不同情形，取消其直接负责的董事、高级管理人员一定期限直至终身的任职资格，禁止直接负责的董事、高级管理人员和其他直接责任人员一定期限直至终身从事银行业工作。

商业银行的行为尚不构成犯罪的，对直接负责的董事、高级管理人员和其他直接责任人员，给予警告，处五万元以上五十万元以下罚款。

第九十条 商业银行及其工作人员对国务院银行业监督管理机构、中国人民银行的处罚决定不服的，可以依照《中华人民共和国行政诉讼法》的规定向人民法院提起诉讼。

（二）行政法规

个人存款账户实名制规定

基本信息：	
【发布机关】国务院	【时效性】现行有效
【发文字号】国务院令第 285 号	【效力级别】行政法规
【发布日期】2000.3.20	【实施日期】2000.4.1

个人存款账户实名制规定

第一条　为了保证个人存款账户的真实性，维护存款人的合法权益，制定本规定。

第二条　中华人民共和国境内的金融机构和在金融机构开立个人存款账户的个人，应当遵守本规定。

第三条　本规定所称金融机构，是指在境内依法设立和经营个人存款业务的机构。

第四条　本规定所称个人存款账户，是指个人在金融机构开立的人民币、外币存款账户，包括活期存款账户、定期存款账户、定活两便存款账户、通知存款账户以及其他形式的个人存款账户。

第五条　本规定所称实名，是指符合法律、行政法规和国家有关规定的身份证件上使用的姓名。

下列身份证件为实名证件：

（一）居住在境内的中国公民，为居民身份证或者临时居民身份证；

（二）居住在境内的１６周岁以下的中国公民，为户口簿；

（三）中国人民解放军军人，为军人身份证件；中国人民武装警察，为武装警察身份证件；

（四）香港、澳门居民，为港澳居民往来内地通行证；台湾居民，为台湾居民来往大陆通行证或者其他有效旅行证件；

（五）外国公民，为护照。

前款未作规定的，依照有关法律、行政法规和国家有关规定执行。

第六条　个人在金融机构开立个人存款账户时，应当出示本人身份证件，使用实名。

代理他人在金融机构开立个人存款账户的，代理人应当出示被代理人和代理人的身份证件。

第七条　在金融机构开立个人存款账户的，金融机构应当要求其出示本人身份证件，

进行核对，并登记其身份证件上的姓名和号码。代理他人在金融机构开立个人存款账户的，金融机构应当要求其出示被代理人和代理人的身份证件，进行核对，并登记被代理人和代理人的身份证件上的姓名和号码。

不出示本人身份证件或者不使用本人身份证件上的姓名的，金融机构不得为其开立个人存款账户。

第八条　金融机构及其工作人员负有为个人存款账户的情况保守秘密的责任。

金融机构不得向任何单位或者个人提供有关个人存款账户的情况，并有权拒绝任何单位或者个人查询、冻结、扣划个人在金融机构的款项；但是，法律另有规定的除外。

第九条　金融机构违反本规定第七条规定的，由中国人民银行给予警告，可以处１０００元以上５０００元以下的罚款；情节严重的，可以并处责令停业整顿，对直接负责的主管人员和其他直接责任人员依法给予纪律处分；构成犯罪的，依法追究刑事责任。

第十条　本规定施行前，已经在金融机构开立的个人存款账户，按照本规定施行前国家有关规定执行；本规定施行后，在原账户办理第一笔个人存款时，原账户没有使用实名的，应当依照本规定使用实名。

第十一条　本规定由中国人民银行组织实施。

第十二条　本规定自２０００年４月１日起施行。

征信业管理条例

基本信息：	
【发布机关】国务院	【时效性】 现行有效
【发文字号】国务院令第 631 号	【效力级别】行政法规
【发布日期】2013.1.21	【实施日期】2013.3.15

征信业管理条例

第一章　总 则

第一条　为了规范征信活动，保护当事人合法权益，引导、促进征信业健康发展，推进社会信用体系建设，制定本条例。

第二条　在中国境内从事征信业务及相关活动，适用本条例。

本条例所称征信业务，是指对企业、事业单位等组织（以下统称企业）的信用信息和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

国家设立的金融信用信息基础数据库进行信息的采集、整理、保存、加工和提供，适用本条例第五章规定。

国家机关以及法律、法规授权的具有管理公共事务职能的组织依照法律、行政法规和国务院的规定，为履行职责进行的企业和个人信息的采集、整理、保存、加工和公布，不适用本条例。

第三条　从事征信业务及相关活动，应当遵守法律法规，诚实守信，不得危害国家秘密，不得侵犯商业秘密和个人隐私。

第四条　中国人民银行（以下称国务院征信业监督管理部门）及其派出机构依法对征信业进行监督管理。

县级以上地方人民政府和国务院有关部门依法推进本地区、本行业的社会信用体系建设，培育征信市场，推动征信业发展。

第二章　征信机构

第五条　本条例所称征信机构，是指依法设立，主要经营征信业务的机构。

第六条　设立经营个人征信业务的征信机构，应当符合《中华人民共和国公司法》规定的公司设立条件和下列条件，并经国务院征信业监督管理部门批准：

（一）主要股东信誉良好，最近 3 年无重大违法违规记录；

（二）注册资本不少于人民币 5000 万元；

（三）有符合国务院征信业监督管理部门规定的保障信息安全的设施、设备和制度、措施；

（四）拟任董事、监事和高级管理人员符合本条例第八条规定的任职条件；

（五）国务院征信业监督管理部门规定的其他审慎性条件。

第七条　申请设立经营个人征信业务的征信机构，应当向国务院征信业监督管理部门提交申请书和证明其符合本条例第六条规定条件的材料。

国务院征信业监督管理部门应当依法进行审查，自受理申请之日起 60 日内作出批准或者不予批准的决定。决定批准的，颁发个人征信业务经营许可证；不予批准的，应当书面说明理由。

经批准设立的经营个人征信业务的征信机构，凭个人征信业务经营许可证向公司登记机关办理登记。

未经国务院征信业监督管理部门批准，任何单位和个人不得经营个人征信业务。

第八条　经营个人征信业务的征信机构的董事、监事和高级管理人员，应当熟悉与征

信业务相关的法律法规，具有履行职责所需的征信业从业经验和管理能力，最近 3 年无重大违法违规记录，并取得国务院征信业监督管理部门核准的任职资格。

第九条　经营个人征信业务的征信机构设立分支机构、合并或者分立、变更注册资本、变更出资额占公司资本总额 5%以上或者持股占公司股份 5%以上的股东的，应当经国务院征信业监督管理部门批准。

经营个人征信业务的征信机构变更名称的，应当向国务院征信业监督管理部门办理备案。

第十条　设立经营企业征信业务的征信机构，应当符合《中华人民共和国公司法》规定的设立条件，并自公司登记机关准予登记之日起 30 日内向所在地的国务院征信业监督管理部门派出机构办理备案，并提供下列材料：

（一）营业执照；

（二）股权结构、组织机构说明；

（三）业务范围、业务规则、业务系统的基本情况；

（四）信息安全和风险防范措施。

备案事项发生变更的，应当自变更之日起 30 日内向原备案机构办理变更备案。

第十一条　征信机构应当按照国务院征信业监督管理部门的规定，报告上一年度开展征信业务的情况。

国务院征信业监督管理部门应当向社会公告经营个人征信业务和企业征信业务的征信机构名单，并及时更新。

第十二条　征信机构解散或者被依法宣告破产的，应当向国务院征信业监督管理部门报告，并按照下列方式处理信息数据库：

（一）与其他征信机构约定并经国务院征信业监督管理部门同意，转让给其他征信机构；

（二）不能依照前项规定转让的，移交给国务院征信业监督管理部门指定的征信机构；

（三）不能依照前两项规定转让、移交的，在国务院征信业监督管理部门的监督下销毁。

经营个人征信业务的征信机构解散或者被依法宣告破产的，还应当在国务院征信业监督管理部门指定的媒体上公告，并将个人征信业务经营许可证交国务院征信业监督管理部门注销。

第三章　征信业务规则

第十三条　采集个人信息应当经信息主体本人同意，未经本人同意不得采集。但是，依照法律、行政法规规定公开的信息除外。

企业的董事、监事、高级管理人员与其履行职务相关的信息，不作为个人信息。

第十四条　禁止征信机构采集个人的宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规规定禁止采集的其他个人信息。

征信机构不得采集个人的收入、存款、有价证券、商业保险、不动产的信息和纳税数额信息。但是，征信机构明确告知信息主体提供该信息可能产生的不利后果，并取得其书面同意的除外。

第十五条　信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人。但是，依照法律、行政法规规定公开的不良信息除外。

第十六条　征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为5年；超过 5年的，应当予以删除。

在不良信息保存期限内，信息主体可以对不良信息作出说明，征信机构应当予以记载。

第十七条　信息主体可以向征信机构查询自身信息。个人信息主体有权每年两次免费获取本人的信用报告。

第十八条　向征信机构查询个人信息的，应当取得信息主体本人的书面同意并约定用途。但是，法律规定可以不经同意查询的除外。

征信机构不得违反前款规定提供个人信息。

第十九条　征信机构或者信息提供者、信息使用者采用格式合同条款取得个人信息主体同意的，应当在合同中作出足以引起信息主体注意的提示，并按照信息主体的要求作出明确说明。

第二十条　信息使用者应当按照与个人信息主体约定的用途使用个人信息，不得用作约定以外的用途，不得未经个人信息主体同意向第三方提供。

第二十一条　征信机构可以通过信息主体、企业交易对方、行业协会提供信息，政府有关部门依法已公开的信息，人民法院依法公布的判决、裁定等渠道，采集企业信息。

征信机构不得采集法律、行政法规禁止采集的企业信息。

第二十二条　征信机构应当按照国务院征信业监督管理部门的规定，建立健全和严格执行保障信息安全的规章制度，并采取有效技术措施保障信息安全。

经营个人征信业务的征信机构应当对其工作人员查询个人信息的权限和程序作出明确规定，对工作人员查询个人信息的情况进行登记，如实记载查询工作人员的姓名，查询的

时间、内容及用途。工作人员不得违反规定的权限和程序查询信息，不得泄露工作中获取的信息。

第二十三条　征信机构应当采取合理措施，保障其提供信息的准确性。

征信机构提供的信息供信息使用者参考。

第二十四条　征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。

征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。

第四章　异议和投诉

第二十五条　信息主体认为征信机构采集、保存、提供的信息存在错误、遗漏的，有权向征信机构或者信息提供者提出异议，要求更正。

征信机构或者信息提供者收到异议，应当按照国务院征信业监督管理部门的规定对相关信息作出存在异议的标注，自收到异议之日起 20 日内进行核查和处理，并将结果书面答复异议人。

经核查，确认相关信息确有错误、遗漏的，信息提供者、征信机构应当予以更正；确认不存在错误、遗漏的，应当取消异议标注；经核查仍不能确认的，对核查情况和异议内容应当予以记载。

第二十六条　信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以向所在地的国务院征信业监督管理部门派出机构投诉。

受理投诉的机构应当及时进行核查和处理，自受理之日起 30 日内书面答复投诉人。

信息主体认为征信机构或者信息提供者、信息使用者侵害其合法权益的，可以直接向人民法院起诉。

第五章　金融信用信息基础数据库

第二十七条　国家设立金融信用信息基础数据库，为防范金融风险、促进金融业发展提供相关信息服务。

金融信用信息基础数据库由专业运行机构建设、运行和维护。该运行机构不以营利为目的，由国务院征信业监督管理部门监督管理。

第二十八条　金融信用信息基础数据库接收从事信贷业务的机构按照规定提供的信贷信息。

金融信用信息基础数据库为信息主体和取得信息主体本人书面同意的信息使用者提供

查询服务。国家机关可以依法查询金融信用信息基础数据库的信息。

第二十九条　从事信贷业务的机构应当按照规定向金融信用信息基础数据库提供信贷信息。

从事信贷业务的机构向金融信用信息基础数据库或者其他主体提供信贷信息，应当事先取得信息主体的书面同意，并适用本条例关于信息提供者的规定。

第三十条　不从事信贷业务的金融机构向金融信用信息基础数据库提供、查询信用信息以及金融信用信息基础数据库接收其提供的信用信息的具体办法，由国务院征信业监督管理部门会同国务院有关金融监督管理机构依法制定。

第三十一条　金融信用信息基础数据库运行机构可以按照补偿成本原则收取查询服务费用，收费标准由国务院价格主管部门规定。

第三十二条　本条例第十四条、第十六条、第十七条、第十八条、第二十二条、第二十三条、第二十四条、第二十五条、第二十六条适用于金融信用信息基础数据库运行机构。

第六章　监督管理

第三十三条　国务院征信业监督管理部门及其派出机构依照法律、行政法规和国务院的规定，履行对征信业和金融信用信息基础数据库运行机构的监督管理职责，可以采取下列监督检查措施：

（一）进入征信机构、金融信用信息基础数据库运行机构进行现场检查，对向金融信用信息基础数据库提供或者查询信息的机构遵守本条例有关规定的情况进行检查；

（二）询问当事人和与被调查事件有关的单位和个人，要求其对与被调查事件有关的事项作出说明；

（三）查阅、复制与被调查事件有关的文件、资料，对可能被转移、销毁、隐匿或者篡改的文件、资料予以封存；

（四）检查相关信息系统。

进行现场检查或者调查的人员不得少于 2 人，并应当出示合法证件和检查、调查通知书。

被检查、调查的单位和个人应当配合，如实提供有关文件、资料，不得隐瞒、拒绝和阻碍。

第三十四条　经营个人征信业务的征信机构、金融信用信息基础数据库、向金融信用信息基础数据库提供或者查询信息的机构发生重大信息泄露等事件的，国务院征信业监督管理部门可以采取临时接管相关信息系统等必要措施，避免损害扩大。

第三十五条　国务院征信业监督管理部门及其派出机构的工作人员对在工作中知悉的国家秘密和信息主体的信息，应当依法保密。

第七章　法律责任

第三十六条　未经国务院征信业监督管理部门批准，擅自设立经营个人征信业务的征信机构或者从事个人征信业务活动的，由国务院征信业监督管理部门予以取缔，没收违法所得，并处 5 万元以上 50 万元以下的罚款；构成犯罪的，依法追究刑事责任。

第三十七条　经营个人征信业务的征信机构违反本条例第九条规定的，由国务院征信业监督管理部门责令限期改正，对单位处 2 万元以上 20 万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警告，处 1 万元以下的罚款。

经营企业征信业务的征信机构未按照本条例第十条规定办理备案的，由其所在地的国务院征信业监督管理部门派出机构责令限期改正；逾期不改正的，依照前款规定处罚。

第三十八条　征信机构、金融信用信息基础数据库运行机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处 5 万元以上 50 万元以下的罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

（一）窃取或者以其他方式非法获取信息；

（二）采集禁止采集的个人信息或者未经同意采集个人信息；

（三）违法提供或者出售信息；

（四）因过失泄露信息；

（五）逾期不删除个人不良信息；

（六）未按照规定对异议信息进行核查和处理；

（七）拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料；

（八）违反征信业务规则，侵害信息主体合法权益的其他行为。

经营个人征信业务的征信机构有前款所列行为之一，情节严重或者造成严重后果的，由国务院征信业监督管理部门吊销其个人征信业务经营许可证。

第三十九条　征信机构违反本条例规定，未按照规定报告其上一年度开展征信业务情况的，由国务院征信业监督管理部门或者其派出机构责令限期改正；逾期不改正的，对单位处 2 万元以上 10 万元以下的罚款；对直接负责的主管人员和其他直接责任人员给予警

告，处 1 万元以下的罚款。

第四十条　向金融信用信息基础数据库提供或者查询信息的机构违反本条例规定，有下列行为之一的，由国务院征信业监督管理部门或者其派出机构责令限期改正，对单位处 5 万元以上 50 万元以下的罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任：

（一）违法提供或者出售信息；

（二）因过失泄露信息；

（三）未经同意查询个人信息或者企业的信贷信息；

（四）未按照规定处理异议或者对确有错误、遗漏的信息不予更正；

（五）拒绝、阻碍国务院征信业监督管理部门或者其派出机构检查、调查或者不如实提供有关文件、资料。

第四十一条　信息提供者违反本条例规定，向征信机构、金融信用信息基础数据库提供非依法公开的个人不良信息，未事先告知信息主体本人，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处 2 万元以上 20 万元以下的罚款；对个人处 1 万元以上 5 万元以下的罚款。

第四十二条　信息使用者违反本条例规定，未按照与个人信息主体约定的用途使用个人信息或者未经个人信息主体同意向第三方提供个人信息，情节严重或者造成严重后果的，由国务院征信业监督管理部门或者其派出机构对单位处 2 万元以上 20 万元以下的罚款；对个人处 1 万元以上 5 万元以下的罚款；有违法所得的，没收违法所得。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第四十三条　国务院征信业监督管理部门及其派出机构的工作人员滥用职权、玩忽职守、徇私舞弊，不依法履行监督管理职责，或者泄露国家秘密、信息主体信息的，依法给予处分。给信息主体造成损失的，依法承担民事责任；构成犯罪的，依法追究刑事责任。

第八章　附则

第四十四条　本条例下列用语的含义：

（一）信息提供者，是指向征信机构提供信息的单位和个人，以及向金融信用信息基础数据库提供信息的单位。

（二）信息使用者，是指从征信机构和金融信用信息基础数据库获取信息的单位和个人。

（三）不良信息，是指对信息主体信用状况构成负面影响的下列信息：信息主体在借贷、赊购、担保、租赁、保险、使用信用卡等活动中未按照合同履行义务的信息，对信息主体的行政处罚信息，人民法院判决或者裁定信息主体履行义务以及强制执行的信息，以及国务院征信业监督管理部门规定的其他不良信息。

第四十五条　外商投资征信机构的设立条件，由国务院征信业监督管理部门会同国务院有关部门制定，报国务院批准。

境外征信机构在境内经营征信业务，应当经国务院征信业监督管理部门批准。

第四十六条　本条例施行前已经经营个人征信业务的机构，应当自本条例施行之日起6个月内，依照本条例的规定申请个人征信业务经营许可证。

本条例施行前已经经营企业征信业务的机构，应当自本条例施行之日起 3个月内，依照本条例的规定办理备案。

第四十七条　本条例自 2013 年 3月 15 日起施行。

（三）部门规章

个人信用信息基础数据库管理暂行办法

基本信息：

【发布机关】中国人民银行

【时效性】现行有效

【发文字号】中国人民银行令〔2005〕第3号

【效力级别】部门规章

【发布日期】2005.8.18

【实施日期】2005.10.01

个人信用信息基础数据库管理暂行办法

第一章　总则

第一条　为维护金融稳定，防范和降低商业银行的信用风险，促进个人信贷业务的发展，保障个人信用信息的安全和合法使用，根据《中华人民共和国中国人民银行法》等有关法律规定，制定本办法。

第二条　中国人民银行负责组织商业银行建立个人信用信息基础数据库（以下简称个人信用数据库），并负责设立征信服务中心，承担个人信用数据库的日常运行和管理。

第三条　个人信用数据库采集、整理、保存个人信用信息，为商业银行和个人提供信用报告查询服务，为货币政策制定、金融监管和法律、法规规定的其他用途提供有关信息服务。

第四条　本办法所称个人信用信息包括个人基本信息、个人信贷交易信息以及反映个人信用状况的其他信息。

前款所称个人基本信息是指自然人身份识别信息、职业和居住地址等信息；个人信贷交易信息是指商业银行提供的自然人在个人贷款、贷记卡、准贷记卡、担保等信用活动中形成的交易记录；反映个人信用状况的其他信息是指除信贷交易信息之外的反映个人信用状况的相关信息。

第五条　中国人民银行、商业银行及其工作人员应当为在工作中知悉的个人信用信息保密。

第二章　报送和整理

第六条　商业银行应当遵守中国人民银行发布的个人信用数据库标准及其有关要求，准确、完整、及时地向个人信用数据库报送个人信用信息。

第七条　商业银行不得向未经信贷征信主管部门批准建立或变相建立的个人信用数据库提供个人信用信息。

第八条　征信服务中心应当建立完善的规章制度和采取先进的技术手段确保个人信用信息安全。

第九条　征信服务中心根据生成信用报告的需要，对商业银行报送的个人信用信息进行客观整理、保存，不得擅自更改原始数据。

第十条　征信服务中心认为有关商业银行报送的信息可疑时，应当按有关规定的程序及时向该商业银行发出复核通知。

商业银行应当在收到复核通知之日起 5 个工作日内给予答复。

第十一条　商业银行发现其所报送的个人信用信息不准确时，应当及时报告征信服务中心，征信服务中心收到纠错报告应当立即进行更正。

第三章　查询

第十二条　商业银行办理下列业务，可以向个人信用数据库查询个人信用报告：

（一）审核个人贷款申请的；

（二）审核个人贷记卡、准贷记卡申请的；

（三）审核个人作为担保人的；

（四）对已发放的个人信贷进行贷后风险管理的；

（五）受理法人或其他组织的贷款申请或其作为担保人，需要查询其法定代表人及出资人信用状况的。

第十三条　除本办法第十二条第（四）项规定之外，商业银行查询个人信用报告时应当取得被查询人的书面授权。书面授权可以通过在贷款、贷记卡、准贷记卡以及担保申请书中增加相应条款取得。

第十四条　商业银行应当制定贷后风险管理查询个人信用报告的内部授权制度和查询管理程序。

第十五条　征信服务中心可以根据个人申请有偿提供其本人信用报告。

征信服务中心应当制定相应的处理程序，核实申请人身份。

第四章　异议处理

第十六条　个人认为本人信用报告中的信用信息存在错误（以下简称异议信息）时，可以通过所在地中国人民银行征信管理部门或直接向征信服务中心提出书面异议申请。

中国人民银行征信管理部门应当在收到异议申请的 2 个工作日内将异议申请转交征信服务中心。

第十七条　征信服务中心应当在接到异议申请的 2 个工作日内进行内部核查。

征信服务中心发现异议信息是由于个人信用数据库信息处理过程造成的，应当立即进行更正，并检查个人信用数据库处理程序和操作规程存在的问题。

第十八条　征信服务中心内部核查未发现个人信用数据库处理过程存在问题的，应当立即书面通知提供相关信息的商业银行进行核查。

第十九条　商业银行应当在接到核查通知的 10 个工作日内向征信服务中心作出核查情况的书面答复。异议信息确实有误的，商业银行应当采取以下措施：

（一）应当向征信服务中心报送更正信息；

（二）检查个人信用信息报送的程序；

（三）对后续报送的其他个人信用信息进行检查，发现错误的，应当重新报送。

第二十条　征信服务中心收到商业银行重新报送的更正信息后，应当在 2 个工作日内对异议信息进行更正。

异议信息确实有误，但因技术原因暂时无法更正的，征信服务中心应当对该异议信息作特殊标注，以有别于其他异议信息。

第二十一条　经过核查，无法确认异议信息存在错误的，征信服务中心不得按照异议申请人要求更改相关个人信用信息。

第二十二条　征信服务中心应当在接受异议申请后 15 个工作日内，向异议申请人或转交异议申请的中国人民银行征信管理部门提供书面答复；异议信息得到更正的，征信服务中心同时提供更正后的信用报告。

异议信息确实有误，但因技术原因暂时无法更正异议信息的，征信服务中心应当在书面答复中予以说明，待异议信息更正后，提供更正后的信用报告。

第二十三条　转交异议申请的中国人民银行征信管理部门应当自接到征信服务中心书面答复和更正后的信用报告之日起 2 个工作日内，向异议申请人转交。

第二十四条　对于无法核实的异议信息，征信服务中心应当允许异议申请人对有关异议信息附注 100 字以内的个人声明。个人声明不得包含与异议信息无关的内容，异议申请人应当对个人声明的真实性负责。

征信服务中心应当妥善保存个人声明原始档案，并将个人声明载入异议人信用报告。

第二十五条　征信服务中心应当对处于异议处理期的信息予以标注。

第五章　安全管理

第二十六条　商业银行应当根据中国人民银行的有关规定，制定相关信用信息报送、

查询、使用、异议处理、安全管理等方面的内部管理制度和操作规程，并报中国人民银行备案。

第二十七条　商业银行应当建立用户管理制度，明确管理员用户、数据上报用户和信息查询用户的职责及操作规程。

商业银行管理员用户、数据上报用户和查询用户不得互相兼职。

第二十八条　商业银行管理员用户应当根据操作规程，为得到相关授权的人员创建相应用户。管理员用户不得直接查询个人信用信息。

管理员用户应当加强对同级查询用户、数据上报用户与下一级管理员用户的日常管理。查询用户工作人员调离，该用户应当立即予以停用。

第二十九条　商业银行管理员用户、数据上报用户和查询用户须报中国人民银行征信管理部门和征信服务中心备案。

前款用户工作人员发生变动，商业银行应当在 2个工作日内向中国人民银行征信管理部门和征信服务中心变更备案。

第三十条　商业银行应当制定管理员用户和查询用户的口令控制制度，并定期检查口令控制执行情况。

第三十一条　商业银行应当建立保证个人信用信息安全的管理制度，确保只有得到内部授权的人员才能接触个人信用报告，不得将个人信用报告用于本办法第十二条规定以外的其它用途。

第三十二条　征信服务中心应当制定信用信息采集、整理、保存、查询、异议处理、用户管理、安全管理等方面的管理制度和操作规程，明确岗位职责，完善内控制度，保障个人信用数据库的正常运行和个人信用信息的安全。

第三十三条　征信服务中心及其工作人员不得违反法律、法规及本办法的规定，篡改、毁损、泄露或非法使用个人信用信息，不得与自然人、法人、其它组织恶意串通，提供虚假信用报告。

第三十四条　征信服务中心应当建立个人信用数据库内部运行和外部访问的监控制度，监督个人信用数据库用户和商业银行用户的操作，防范对个人信用数据库的非法入侵。

第三十五条　征信服务中心应当建立灾难备份系统，采取必要的安全保障措施，防止系统数据丢失。

第三十六条　征信服务中心应当对商业银行的所有查询进行记录，并及时向商业银行反馈。

第三十七条　商业银行应当经常对个人信用数据库的查询情况进行检查，确保所有查询符合本办法的规定，并定期向中国人民银行及征信服务中心报告查询检查结果。

征信服务中心应当定期核查商业银行对个人信用数据库的查询情况。

第六章　罚则

第三十八条　商业银行未按照本办法规定建立相应管理制度及操作规程的，由中国人民银行责令改正，逾期不改正的，给予警告，并处以三万元罚款。

第三十九条　商业银行有下列情形之一的，由中国人民银行责令改正，并处一万元以上三万元以下罚款；涉嫌犯罪的，依法移交司法机关处理：

（一）违反本办法规定，未准确、完整、及时报送个人信用信息的；

（二）违反本办法第七条规定的；

（三）越权查询个人信用数据库的；

（四）将查询结果用于本办法规定之外的其他目的的；

（五）违反异议处理规定的；

（六）违反本办法安全管理要求的。

第四十条　商业银行有本办法第三十八条至第三十九条规定情形的，中国人民银行可以建议商业银行对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分；涉嫌犯罪的，依法移交司法机关处理。

第四十一条　征信服务中心工作人员有下列情形之一的，由中国人民银行依法给予行政处分；涉嫌犯罪的，依法移交司法机关处理：

（一）违反本办法规定，篡改、毁损、泄露或非法使用个人信用信息的；

（二）与自然人、法人、其它组织恶意串通，提供虚假信用报告的。

第四十二条　中国人民银行其他工作人员有违反本办法规定的行为，造成个人信用信息被泄露的，依法给予行政处分；涉嫌犯罪的，依法移交司法机关处理。

第七章　附则

第四十三条　本办法所称商业银行，是指在中华人民共和国境内设立的商业银行、城市信用合作社、农村信用合作社以及经国务院银行业监督管理机构批准的专门从事信贷业务的其他金融机构。

第四十四条　本办法由中国人民银行负责解释。

第四十五条　本办法自 2005 年 10 月 1 日起施行。

电子银行业务管理办法

基本信息：	
【发布机关】中国银行业监督管理委员会	【时效性】现行有效
【发文字号】银监会令〔2006〕第 5 号	【效力级别】部门规章
【发布日期】2006.01.26	【实施日期】2006.03.01

电子银行业务管理办法

第一章　总则

第一条　为加强电子银行业务的风险管理，保障客户及银行的合法权益，促进电子银行业务的健康有序发展，根据《中华人民共和国银行业监督管理法》、《中华人民共和国商业银行法》和《中华人民共和国外资金融机构管理条例》等法律法规，制定本办法。

第二条　本办法所称电子银行业务，是指商业银行等银行业金融机构利用面向社会公众开放的通讯通道或开放型公众网络，以及银行为特定自助服务设施或客户建立的专用网络，向客户提供的银行服务。

电子银行业务包括利用计算机和互联网开展的银行业务（以下简称网上银行业务），利用电话等声讯设备和电信网络开展的银行业务（以下简称电话银行业务），利用移动电话和无线网络开展的银行业务（以下简称手机银行业务），以及其他利用电子服务设备和网络，由客户通过自助服务方式完成金融交易的银行业务。

第三条　银行业金融机构和依据《中华人民共和国外资金融机构管理条例》设立的外资金融机构（以下通称为金融机构），应当按照本办法的规定开展电子银行业务。

在中华人民共和国境内设立的金融资产管理公司、信托投资公司、财务公司、金融租赁公司以及经中国银行业监督管理委员会（以下简称中国银监会）批准设立的其他金融机构，开办具有电子银行性质的电子金融业务，适用本办法对金融机构开展电子银行业务的有关规定。

第四条　经中国银监会批准，金融机构可以在中华人民共和国境内开办电子银行业务，向中华人民共和国境内企业、居民等客户提供电子银行服务，也可按照本办法的有关规定开展跨境电子银行服务。

第五条　金融机构应当按照合理规划、统一管理、保障系统安全运行的原则，开展电子银行业务，保证电子银行业务的健康、有序发展。

第六条　金融机构应根据电子银行业务特性，建立健全电子银行业务风险管理体系和内部控制体系，设立相应的管理机构，明确电子银行业务管理的责任，有效地识别、评估、

监测和控制电子银行业务风险。

第七条　中国银监会负责对电子银行业务实施监督管理。

第二章　申请与变更

第八条　金融机构在中华人民共和国境内开办电子银行业务，应当依照本办法的有关规定，向中国银监会申请或报告。

第九条　金融机构开办电子银行业务，应当具备下列条件：

（一）金融机构的经营活动正常，建立了较为完善的风险管理体系和内部控制制度，在申请开办电子银行业务的前一年内，金融机构的主要信息管理系统和业务处理系统没有发生过重大事故；

（二）制定了电子银行业务的总体发展战略、发展规划和电子银行安全策略，建立了电子银行业务风险管理的组织体系和制度体系；

（三）按照电子银行业务发展规划和安全策略，建立了电子银行业务运营的基础设施和系统，并对相关设施和系统进行了必要的安全检测和业务测试；

（四）对电子银行业务风险管理情况和业务运营设施与系统等，进行了符合监管要求的安全评估；

（五）建立了明确的电子银行业务管理部门，配备了合格的管理人员和技术人员；

（六）中国银监会要求的其他条件。

第十条　金融机构开办以互联网为媒介的网上银行业务、手机银行业务等电子银行业务，除应具备第九条所列条件外，还应具备以下条件：

（一）电子银行基础设施设备能够保障电子银行的正常运行；

（二）电子银行系统具备必要的业务处理能力，能够满足客户适时业务处理的需要；

（三）建立了有效的外部攻击侦测机制；

（四）中资银行业金融机构的电子银行业务运营系统和业务处理服务器设置在中华人民共和国境内；

（五）外资金融机构的电子银行业务运营系统和业务处理服务器可以设置在中华人民共和国境内或境外。设置在境外时，应在中华人民共和国境内设置可以记录和保存业务交易数据的设施设备，能够满足金融监管部门现场检查的要求，在出现法律纠纷时，能够满足中国司法机构调查取证的要求。

第十一条　外资金融机构开办电子银行业务，除应具备第九条、第十条　所列条件外，还应当按照法律、行政法规的有关规定，在中华人民共和国境内设有营业性机构，其所在

国家（地区）监管当局具备对电子银行业务进行监管的法律框架和监管能力。

第十二条　金融机构申请开办电子银行业务，根据电子银行业务的不同类型，分别适用审批制和报告制。

（一）利用互联网等开放性网络或无线网络开办的电子银行业务，包括网上银行、手机银行和利用掌上电脑等个人数据辅助设备开办的电子银行业务，适用审批制；

（二）利用境内或地区性电信网络、有线网络等开办的电子银行业务，适用报告制；

（三）利用银行为特定自助服务设施或与客户建立的专用网络开办的电子银行业务，法律法规和行政规章另有规定的遵照其规定，没有规定的适用报告制。

金融机构开办电子银行业务后，与其特定客户建立直接网络连接提供相关服务，属于电子银行日常服务，不属于开办电子银行业务申请的类型。

第十三条　金融机构申请开办需要审批的电子银行业务之前，应先就拟申请的业务与中国银监会进行沟通，说明拟申请的电子银行业务系统和基础设施设计、建设方案，以及基本业务运营模式等，并根据沟通情况，对有关方案进行调整。

进行监管沟通后，金融机构应根据调整完善后的方案开展电子银行系统建设，并应在申请前完成对相关系统的内部测试工作。

内部测试对象仅限于金融机构内部人员、外包机构相关工作人员和相关机构的工作人员，不得扩展到一般客户。

第十四条　金融机构申请开办电子银行业务时，可以在一个申请报告中同时申请不同类型的电子银行业务，但在申请中应注明所申请的电子银行业务类型。

第十五条　金融机构向中国银监会或其派出机构申请开办电子银行业务，应提交以下文件、资料（一式三份）：

（一）由金融机构法定代表人签署的开办电子银行业务的申请报告；

（二）拟申请的电子银行业务类型及拟开展的业务种类；

（三）电子银行业务发展规划；

（四）电子银行业务运营设施与技术系统介绍；

（五）电子银行业务系统测试报告；

（六）电子银行安全评估报告；

（七）电子银行业务运行应急计划和业务连续性计划；

（八）电子银行业务风险管理体系及相应的规章制度；

（九）电子银行业务的管理部门、管理职责，以及主要负责人介绍；

（十）申请单位联系人以及联系电话、传真、电子邮件信箱等联系方式；

（十一）中国银监会要求提供的其他文件和资料。

第十六条　中国银监会或其派出机构在收到金融机构的有关申请材料后，根据监管需要，要求商业银行补充材料时，应一次性将有关要求告知金融机构。

金融机构应根据中国银监会或其派出机构的要求，重新编制和装订申请材料，并更正材料递交日期。

第十七条　中国银监会或其派出机构在收到金融机构申请开办需要审批的电子银行业务完整申请材料 3 个月内，作出批准或者不批准的书面决定；决定不批准的，应当说明理由。

第十八条　金融机构在一份申请报告中申请了多个类型的电子银行业务时，中国银监会或其派出机构可以根据有关规定和要求批准全部或部分电子银行业务类型的申请。

对于中国银监会或其派出机构未批准的电子银行业务类型，金融机构可按有关规定重新申请。

第十九条　金融机构开办适用于报告制的电子银行业务类型，不需申请，但应参照第十五条的有关规定，在开办电子银行业务之前 1 个月，将相关材料报送中国银监会或其派出机构。

第二十条　金融机构开办电子银行业务后，可以利用电子银行平台进行传统银行产品和服务的宣传、销售，也可以根据电子银行业务的特点开发新的业务类型。

金融机构利用电子银行平台宣传有关银行产品或服务时，应当遵守相关法律法规和业务管理规章的有关规定。利用电子银行平台销售有关银行产品或服务时，应认真分析选择适应电子银行销售的产品，不得利用电子银行销售需要对客户进行当面评估后才能销售的，或者需要客户当面确认才能销售的银行产品，法律法规和行政规章另有规定的除外。

第二十一条　金融机构根据业务发展需要，增加或变更电子银行业务类型，适用审批制或报告制。

第二十二条　金融机构增加或者变更以下电子银行业务类型，适用审批制：

（一）有关法律法规和行政规章规定需要审批但金融机构尚未申请批准，并准备利用电子银行开办的；

（二）金融机构将已获批准的业务应用于电子银行时，需要与证券业、保险业相关机构进行直接实时数据交换才能实施的；

（三）金融机构之间通过互联电子银行平台联合开展的；

（四）提供跨境电子银行服务的。

第二十三条　金融机构增加或变更需要审批的电子银行业务类型，应向中国银监会或其派出机构报送以下文件和资料（一式三份）：

（一）由金融机构法定代表人签署的增加或变更业务类型的申请；

（二）拟增加或变更业务类型的定义和操作流程；

（三）拟增加或变更业务类型的风险特征和防范措施；

（四）有关管理规章制度；

（五）申请单位联系人以及联系电话、传真、电子邮件信箱等联系方式；

（六）中国银监会要求提供的其他文件和资料。

第二十四条　业务经营活动不受地域限制的银行业金融机构（以下简称全国性金融机构），申请开办电子银行业务或增加、变更需要审批的电子银行业务类型，应由其总行（公司）统一向中国银监会申请。

按照有关规定只能在某一城市或地区内从事业务经营活动的银行业金融机构（以下简称地区性金融机构），申请开办电子银行业务或增加、变更需要审批的电子银行业务类型，应由其法人机构向所在地中国银监会派出机构申请。

外资金融机构申请开办电子银行业务或增加、变更需要审批的电子银行业务类型，应由其总行（公司）或在中华人民共和国境内的主报告行向中国银监会申请。

第二十五条　中国银监会或其派出机构在收到金融机构增加或变更需要审批的电子银行业务类型完整申请材料 3 个月内，做出批准或者不批准的书面决定；决定不批准的，应当说明理由。

第二十六条　其他电子银行业务类型适用报告制，金融机构增加或变更时不需申请，但应在开办该业务类型前 1 个月内，参照第二十三条的有关规定，将有关材料报送中国银监会或其派出机构。

第二十七条　已经实现业务数据集中处理和系统整合（以下简称数据集中处理）的银行业金融机构，获准开办电子银行业务后，可以授权其分支机构开办部分或全部电子银行业务。其分支机构在开办相关业务之前，应向所在地中国银监会派出机构报告。

未实现数据集中处理的银行业金融机构，如果其分支机构的电子银行业务处理系统独立于总部，该分支机构开办电子银行业务按照地区性金融机构开办电子银行业务的情形管理，应持其总行授权文件，按照有关规定向所在地中国银监会派出机构申请或报告。其他

分支机构只需持其总行授权文件，在开办相关业务之前，向所在地中国银监会派出机构报告。

外资金融机构获准开办电子银行业务后，其境内分支机构开办电子银行业务，应持其总行（公司）授权文件向所在地中国银监会派出机构报告。

第二十八条　已开办电子银行业务的金融机构按计划决定终止全部电子银行服务或部分类型的电子银行服务时，应提前 3 个月就终止电子银行服务的原因及相关问题处置方案等，报告中国银监会，并同时予以公告。

金融机构按计划决定停办部分电子银行业务类型时，应于停办该业务前 1 个月内向中国银监会报告，并予以公告。

金融机构终止电子银行服务或停办部分业务类型，必须采取有效的措施保护客户的合法权益，并针对可能出现的问题制定有效的处置方案。

第二十九条　金融机构终止电子银行服务或停办部分业务类型后，需要重新开办电子银行业务或者重新开展已停办的业务类型时，应按照相关规定重新申请或办理。

第三十条　金融机构因电子银行系统升级、调试等原因，需要按计划暂时停止电子银行服务的，应选择适当的时间，尽可能减少对客户的影响，并至少提前 3 天在其网站上予以公告。

受突发事件或偶然因素影响非计划暂停电子银行服务，在正常工作时间内超过 4 个小时或者在正常工作时间外超过 8 个小时的，金融机构应在暂停服务后 24 小时内将有关情况报告中国银监会，并应在事故处理基本结束后 3 日内，将事故原因、影响、补救措施及处理情况等，报告中国银监会。

第三章　风险管理

第三十一条　金融机构应当将电子银行业务风险管理纳入本机构风险管理的总体框架之中，并应根据电子银行业务的运营特点，建立健全电子银行风险管理体系和电子银行安全、稳健运营的内部控制体系。

第三十二条　金融机构的电子银行风险管理体系和内部控制体系应当具有清晰的管理架构、完善的规章制度和严格的内部授权控制机制，能够对电子银行业务面临的战略风险、运营风险、法律风险、声誉风险、信用风险、市场风险等实施有效的识别、评估、监测和控制。

第三十三条　金融机构针对传统业务风险制定的审慎性风险管理原则和措施等，同样适用于电子银行业务，但金融机构应根据电子银行业务环境和运行方式的变化，对原有风险管理制度、规则和程序进行必要的和适当的修正。

第三十四条　金融机构的董事会和高级管理层应根据本机构的总体发展战略和实际经营情况，制订电子银行发展战略和可行的经营投资战略，对电子银行的经营进行持续性的综合效益分析，科学评估电子银行业务对金融机构总体风险的影响。

第三十五条　在制定电子银行发展战略时，金融机构应加强电子银行业务的知识产权保护工作。

第三十六条　金融机构应当针对电子银行不同系统、风险设施、信息和其他资源的重要性及其对电子银行安全的影响进行评估分类，制定适当的安全策略，建立健全风险控制程序和安全操作规程，采取相应的安全管理措施。

对各类安全控制措施应定期检查、测试，并根据实际情况适时调整，保证安全措施的持续有效和及时更新。

第三十七条　金融机构应当保障电子银行运营设施设备，以及安全控制设施设备的安全，对电子银行的重要设施设备和数据，采取适当的保护措施。

（一）有形场所的物理安全控制，必须符合国家有关法律法规和安全标准的要求，对尚没有统一安全标准的有形场所的安全控制，金融机构应确保其制定的安全制度有效地覆盖可能面临的主要风险；

（二）以开放型网络为媒介的电子银行系统，应合理设置和使用防火墙、防病毒软件等安全产品与技术，确保电子银行有足够的反攻击能力、防病毒能力和入侵防护能力；

（三）对重要设施设备的接触、检查、维修和应急处理，应有明确的权限界定、责任划分和操作流程，并建立日志文件管理制度，如实记录并妥善保管相关记录；

（四）对重要技术参数，应严格控制接触权限，并建立相应的技术参数调整与变更机制，并保证在更换关键人员后，能够有效防止有关技术参数的泄漏；

（五）对电子银行管理的关键岗位和关键人员，应实行轮岗和强制性休假制度，建立严格的内部监督管理制度。

第三十八条　金融机构应采用适当的加密技术和措施，保证电子交易数据传输的安全性与保密性，以及所传输交易数据的完整性、真实性和不可否认性。

金融机构采用的数据加密技术应符合国家有关规定，并根据电子银行业务的安全性需要和科技信息技术的发展，定期检查和评估所使用的加密技术和算法的强度，对加密方式进行适时调整。

第三十九条　金融机构应当与客户签订电子银行服务协议或合同，明确双方的权利与义务。

在电子银行服务协议中，金融机构应向客户充分揭示利用电子银行进行交易可能面临的风险，金融机构已经采取的风险控制措施和客户应采取的风险控制措施，以及相关风险的责任承担。

第四十条　金融机构应采取适当的措施和采用适当的技术，识别与验证使用电子银行服务客户的真实、有效身份，并应依照与客户签订的有关协议对客户作业权限、资金转移或交易限额等实施有效管理。

第四十一条　金融机构应当建立相应的机制，搜索、监测和处理假冒或有意设置类似于金融机构的电话、网站、短信号码等信息骗取客户资料的活动。

金融机构发现假冒电子银行的非法活动后，应向公安部门报案，并向中国银监会报告。同时，金融机构应及时在其网站、电话语音提示系统或短信平台上，提醒客户注意。

第四十二条　金融机构应尽可能使用统一的电子银行服务电话、域名、短信号码等，并应在与客户签订的协议中明确客户启动电子银行业务的合法途径、意外事件的处理办法，以及联系方式等。

已实现数据集中处理的银行业金融机构开展网上银行类业务，总行（公司）与其分支机构应使用统一的域名；未实现数据集中处理的银行业金融机构开展网上银行类业务时，应由总行（公司）设置统一的接入站点，在其主页内设置其分支机构网站链接。

第四十三条　金融机构应建立电子银行入侵侦测与入侵保护系统，实时监控电子银行的运行情况，定期对电子银行系统进行漏洞扫描，并建立对非法入侵的甄别、处理和报告机制。

第四十四条　金融机构开展电子银行业务，需要对客户信息和交易信息等使用电子签名或电子认证时，应遵照国家有关法律法规的规定。

金融机构使用第三方认证系统，应对第三方认证机构进行定期评估，保证有关认证安全可靠和具有公信力。

第四十五条　金融机构应定期评估可供客户使用的电子银行资源充足情况，采取必要的措施保障线路接入通畅，保证客户对电子银行服务的可用性。

第四十六条　金融机构应制定电子银行业务连续性计划，保证电子银行业务的连续正常运营。

金融机构电子银行业务连续性计划应充分考虑第三方服务供应商对业务连续性的影响，并应采取适当的预防措施。

第四十七条　金融机构应制定电子银行应急计划和事故处理预案，并定期对这些计划和预案进行测试，以管理、控制和减少意外事件造成的危害。

第四十八条　金融机构应定期对电子银行关键设备和系统进行检测，并详细记录检测情况。

第四十九条　金融机构应明确电子银行管理、运营等各个环节的主要权限、职责和相互监督方式，有效隔离电子银行应用系统、验证系统、业务处理系统和数据库管理系统之间的风险。

第五十条　金融机构应建立健全电子银行业务的内部审计制度，定期对电子银行业务进行审计。

第五十一条　金融机构应采取适当的方法和技术，记录并妥善保存电子银行业务数据，电子银行业务数据的保存期限应符合法律法规的有关要求。

第五十二条　金融机构应采取适当措施，保证电子银行业务符合相关法律法规对客户信息和隐私保护的规定。

第五十三条　金融机构应针对电子银行业务发展与管理的实际情况，制订多层次的培训计划，对电子银行管理人员和业务人员进行持续培训。

第四章　数据交换与转移管理

第五十四条　电子银行业务的数据交换与转移，是指金融机构根据业务发展和管理的需要，利用电子银行平台与外部组织或机构相互交换电子银行业务信息和数据，或者将有关电子银行业务数据转移至外部组织或机构的活动。

第五十五条　金融机构根据业务发展需要，可以与其他开展电子银行业务的金融机构建立电子银行系统数据交换机制，实现电子银行业务平台的直接连接，进行境内实时信息交换和跨行资金转移。

第五十六条　建立电子银行业务数据交换机制的金融机构，或者电子银行平台实现相互连接的金融机构，应当建立联合风险管理委员会，负责协调跨行间的业务风险管理与控制。

所有参加数据交换或电子银行平台连接的金融机构都应参加联合风险管理委员会，共同制定并遵守联合风险管理委员会的规章制度和工作规程。

联合风险管理委员会的规章制度、工作规程、会议纪要和有关决议等，应抄报中国银监会。

第五十七条　金融机构根据业务发展或管理的需要，可以与非银行业金融机构直接交换或转移部分电子银行业务数据。

金融机构向非银行业金融机构交换或转移部分电子银行业务数据时，应签订数据交换

（转移）用途与范围明确、管理职责清晰的书面协议，并明确各方的数据保密责任。

第五十八条　金融机构在确保电子银行业务数据安全并被恰当使用的情况下，可以向非金融机构转移部分电子银行业务数据。

（一）金融机构由于业务外包、系统测试（调试）、数据恢复与救援等为维护电子银行正常安全运营的需要而向非金融机构转移电子银行业务数据的，应当事先签订书面保密合同，并指派专人负责监督有关数据的使用、保管、传递和销毁；

（二）金融机构由于业务拓展、业务合作等需要向非金融机构转移电子银行业务数据的，除应签订书面保密合同和指定专人监督外，还应建立对数据接收方的定期检查制度，一旦发现数据接收方不当使用、保管或传递电子银行业务数据，应立即停止相关数据转移，并应采取必要的措施预防电子银行客户的合法权益受到损害，法律法规另有规定的除外；

（三）金融机构不得向无业务往来的非金融机构转移电子银行业务数据，不得出售电子银行业务数据，不得损害客户权益利用电子银行业务数据谋取利益。

第五十九条　金融机构可以为电子商务经营者提供网上支付平台。为电子商务提供网上支付平台时，金融机构应严格审查合作对象，签订书面合作协议，建立有效监督机制，防范不法机构或人员利用电子银行支付平台从事违法资金转移或其他非法活动。

第六十条　外资金融机构因业务或管理需要确需向境外总行（公司）转移有关电子银行业务数据的，应遵守有关法律法规的规定，采取必要的措施保护客户的合法权益，并遵守有关数据交换和转移的规定。

第六十一条　未经电子银行业务数据转出机构的允许，数据接收机构不得将有关电子银行业务数据向第三方转移。法律法规另有规定的除外。

第五章　业务外包管理

第六十二条　电子银行业务外包，是指金融机构将电子银行部分系统的开发、建设，电子银行业务的部分服务与技术支持，电子银行系统的维护等专业化程度较高的业务工作，委托给外部专业机构承担的活动。

第六十三条　金融机构在进行电子银行业务外包时，应根据实际需要，合理确定外包的原则和范围，认真分析和评估业务外包存在的潜在风险，建立健全有关规章制度，制定相应的风险防范措施。

第六十四条　金融机构在选择电子银行业务外包服务供应商时，应充分审查、评估外包服务供应商的经营状况、财务状况和实际风险控制与责任承担能力，进行必要的尽职调查。

第六十五条　金融机构应当与外包服务供应商签订书面合同，明确双方的权利、义务。

在合同中，应明确规定外包服务供应商的保密义务、保密责任。

第六十六条　金融机构应充分认识外包服务供应商对电子银行业务风险控制的影响，并将其纳入总体安全策略之中。

第六十七条　金融机构应建立完整的业务外包风险评估与监测程序，审慎管理业务外包产生的风险。

第六十八条　电子银行业务外包风险的管理应当符合金融机构的风险管理标准，并应建立针对电子银行业务外包风险的应急计划。

第六十九条　金融机构应与外包服务供应商建立有效的联络、沟通和信息交流机制，并应制定在意外情况下能够实现外包服务供应商顺利变更，保证外包服务不间断的应急预案。

第七十条　金融机构对电子银行业务处理系统、授权管理系统、数据备份系统的总体设计开发，以及其他涉及机密数据管理与传递环节的系统进行外包时，应经过金融机构董事会或者法人代表批准，并应在业务外包实施前向中国银监会报告。

第六章　跨境业务活动管理

第七十一条　电子银行的跨境业务活动，是指开办电子银行业务的金融机构利用境内的电子银行系统，向境外居民或企业提供的电子银行服务活动。

金融机构的境内客户在境外使用电子银行服务，不属于跨境业务活动。

第七十二条　金融机构提供跨境电子银行服务，除应遵守中国法律法规和外汇管理政策等规定外，还应遵守境外居民所在国家（地区）的法律规定。

境外电子银行监管部门对跨境电子银行业务要求审批的，金融机构在提供跨境业务活动之前，应获得境外电子银行监管部门的批准。

第七十三条　金融机构开展跨境电子银行业务，除应按照第二章的有关规定向中国银监会申请外，还应当向中国银监会提供以下文件资料：

（一）跨境电子银行服务的国家（地区），以及该国（地区）对电子银行业务管理的法律规定；

（二）跨境电子银行服务的主要对象及服务内容；

（三）未来三年跨境电子银行业务发展规模、客户规模的分析预测；

（四）跨境电子银行业务法律与合规性分析。

第七十四条　金融机构向客户提供跨境电子银行服务，必须签订相关服务协议。

金融机构与客户的服务协议文本，应当使用中文和客户所在国家或地区（或客户同意

的其他国语言）两种文字，两种文字的文本应具有同等法律效力。

第七章　监督管理

第七十五条　中国银监会依法对电子银行业务实施非现场监管、现场检查和安全监测，对电子银行安全评估实施管理，并对电子银行的行业自律组织进行指导和监督。

第七十六条　开展电子银行业务的金融机构应当建立电子银行业务统计体系，并按照相关规定向中国银监会报送统计数据。

商业银行向中国银监会报送的电子银行业务统计数据、报送办法等，由中国银监会另行制定。

第七十七条　金融机构应定期对电子银行业务发展与管理情况进行自我评估，并应每年编制《电子银行年度评估报告》。

第七十八条　金融机构的《电子银行年度评估报告》应至少包括以下几方面内容：

（一）本年度电子银行业务的发展计划与实际发展情况，以及对本年度电子银行发展状况的分析评价；

（二）本年度电子银行业务经营效益的分析、比较与评价，以及主要业务收入和主要业务的服务价格；

（三）电子银行业务风险管理状况的分析与评估，以及本年度电子银行面临的主要风险；

（四）其他需要说明的重要事项。

第七十九条　金融机构的《电子银行年度评估报告》（一式两份）应于下一年度的 3 月底之前报送中国银监会。

第八十条　金融机构应当建立电子银行业务重大安全事故和风险事件的报告制度，并保持与监管部门的经常性沟通。

对于电子银行系统被恶意攻破并已出现客户或银行损失，电子银行被病毒感染并导致机密资料外泄，以及可能会引发其他金融机构电子银行系统风险的事件，金融机构应在事件发生后 48 小时内向中国银监会报告。

第八十一条　中国银监会根据监管的需要，可以依法对金融机构的电子银行业务实施现场检查，也可以聘请外部专业机构对电子银行业务系统进行安全漏洞扫描、攻击测试等检查。

第八十二条　中国银监会对电子银行业务实施现场检查时，除应按照现场检查的有关规定组成检查组并进行相关业务培训外，还应邀请被检查机构的电子银行业务管理和技术

人员介绍其电子银行系统架构、运营管理模式以及关键设备接触要求。

检查人员在实施现场检查过程中，应当遵守被检查机构电子银行安全管理的有关规定。

第八十三条　金融机构的总行（公司），以及已实现数据集中处理的金融机构分支机构电子银行业务的现场检查，由中国银监会负责；未实现数据集中处理的金融机构的分支机构，外资金融机构的分支机构，以及地区性金融机构电子银行业务的现场检查，由所在地银监局负责。

第八十四条　中国银监会聘用外部专业机构对金融机构电子银行系统进行检查时，应与被委托机构签订书面合同和保密协议，明确规定被委托机构可以使用的技术手段和使用方式，并指派专人全程参与并监督外部机构的监测测试活动。

银监局与拟聘用的外部专业机构签订合同之前，应报请银监会批准。

第八十五条　电子银行安全评估是金融机构开办或持续经营电子银行业务的必要条件，也是金融机构电子银行业务风险管理与监管的重要手段。

金融机构应按照中国银监会的有关规定，定期对电子银行系统进行安全评估，并将其作为电子银行风险管理的重要组成部分。

第八十六条　金融机构电子银行安全评估工作，应当由符合一定资质条件、具备相应评估能力的评估机构实施。

中国银监会负责制定评估机构开展电子银行安全评估业务的资质条件和电子银行安全评估的相关制度，并负责对评估机构参与电子银行安全评估的业务资质进行认定。

第八十七条　中国银监会对评估机构电子银行安全评估业务资质的认定，不作为评估机构开展电子银行安全评估业务的必要条件。

电子银行安全评估机构开展电子银行安全评估业务，如需中国银监会对其资质进行专业认定，应按照有关规定申请办理。

第八十八条　金融机构聘请未经中国银监会认定的安全评估机构实施电子银行安全评估时，应按照中国银监会制定的有关条件和标准选择评估机构，并应于签订评估协议前 4 周将拟聘用机构的有关情况报中国银监会。

第八章　法律责任

第八十九条　金融机构在提供电子银行服务时，因电子银行系统存在安全隐患、金融机构内部违规操作和其他非客户原因等造成损失的，金融机构应当承担相应责任。

因客户有意泄漏交易密码，或者未按照服务协议尽到应尽的安全防范与保密义务造成损失的，金融机构可以根据服务协议的约定免于承担相应责任，但法律法规另有规定的除

外。

第九十条　金融机构未经批准擅自开办电子银行业务，或者未经批准增加或变更需要审批的电子银行业务类型，造成客户损失的，金融机构应承担全部责任。法律法规明确规定应由客户承担的责任除外。

第九十一条　金融机构已经按照有关法律法规和行政规章的要求，尽到了电子银行风险管理和安全管理的相应职责，但因其他金融机构或者其他金融机构的外包服务商失职等原因，造成客户损失的，由其他金融机构承担相应责任，但提供电子银行服务的金融机构有义务协助其客户处理有关事宜。

第九十二条　金融机构开展电子银行业务违反审慎经营规则但尚不构成违法违规，并导致电子银行系统存在较大安全隐患的，中国银监会将责令限期改正；逾期未改正，或者其安全隐患在短时间难以解决的，中国银监会可以区别情形，采取下列措施：

（一）暂停批准增加新的电子银行业务类型；

（二）责令金融机构限制发展新的电子银行客户；

（三）责令调整电子银行管理部门负责人。

第九十三条　金融机构在开展电子银行业务过程中，违反有关法律法规和行政规章的，中国银监会将依据有关法律法规和行政规章的规定予以处罚。

第九章　附则

第九十四条　金融机构利用为特定自助服务设施或客户建立的专用网络提供电子银行业务，有相关业务管理规定的，遵照其规定，但网络安全、技术风险等管理应参照本办法的有关规定执行；没有相关业务规定的，遵照本办法。

第九十五条　本办法实施前，经监管部门批准已经开办网上银行业务的金融机构，其已开办的电子银行业务不需再行审批，但应于本办法实施后 1 个月内将已开办的电子银行业务类型、开办时间、审批文件等相关材料报中国银监会。

本办法实施后，上述机构开办尚未开办的电子银行业务类型，应按本办法的有关规定进行申请或报告。

第九十六条　本办法实施前，已经开办网上银行业务但尚未报批或已经申请但尚未获得监管部门批准的金融机构，其开办的网上银行、手机银行，以及其他以互联网或无线网络为媒介的电子银行业务，应在本办法实施后 6 个月内按本办法提交有关申请；已经递交申请材料的，应按照本办法的要求补充有关材料。

上述机构已经开办适用于报告制的电子银行业务，应于本办法实施后 1 个月内将已开

办的电子银行业务类型、开办时间等报中国银监会。

上述机构新开办其他电子银行业务，应遵照本办法的规定。

第九十七条　本办法实施前，未开办网上银行业务但已开办电话银行业务的金融机构，应于本办法实施后 1 个月内将已开办的电子银行业务类型、开办时间等报中国银监会。

上述机构新开办其他电子银行业务，应遵照本办法的规定。

第九十八条　本办法由中国银监会负责解释。

第九十九条　本办法自 2006 年 3 月 1 日起施行。

企业信用信息基础数据库管理暂行办法(征求意见稿)

基本信息：

【发布机关】中国人民银行　　【时效性】-

【发文字号】中国人民银行公告〔2006〕第 8 号　　【效力级别】部门规章

【发布日期】2006.7.14　　【实施日期】-

企业信用信息基础数据库管理暂行办法(征求意见稿)

第一章　总　则

第一条　为推动社会信用体系建设，维护金融稳定，防范和降低信用风险，促进信贷业务的发展，保障借款人和担保人信用信息的安全和合法使用，根据《中华人民共和国中国人民银行法》等有关法律规定，制定本办法。

第二条　中国人民银行负责组织建立企业信用信息基础数据库（以下简称企业信用数据库），并设立征信中心承担企业信用数据库的运行和管理。

第三条　企业信用数据库采集、整理及保存借款人、担保人信用信息，为金融机构、借款人和担保人提供信用信息服务，为货币政策制定、金融监管、国家宏观调控以及法律、行政法规规定的其他用途提供有关信息服务。

第四条　中国人民银行、征信中心、金融机构、合法信息使用方及其工作人员应当为在工作中知悉的借款人、担保人信用信息保密。

第五条　中国人民银行负责对企业信用数据库有关信用信息报送、查询、使用、异议处理和安全管理等活动实施监督管理。

第六条　金融机构和征信中心应当根据相关法律法规及中国人民银行的有关规定，制

定相关信用信息报送、查询、使用、异议处理、安全管理等方面的内部管理制度，并报中国人民银行备案。

第二章　信用信息的报送和整理

第七条　金融机构应当遵守中国人民银行发布的企业信用数据库标准及其有关要求，准确、完整、及时地向企业信用数据库报送借款人、担保人信用信息。

第八条　金融机构不得向未经信贷征信主管部门批准建立或变相建立的企业信用数据库提供借款人、担保人信用信息。

第九条　金融机构应将当天发生、变化的信贷业务信息于下一个工作日结束前报送企业信用数据库。

第十条　金融机构发现其所报送的借款人、担保人信用信息不准确时，应当重新报送更正信息。

第十一条　征信中心对借款人、担保人信用信息进行客观整理、保存，不得擅自更改原始数据。

第十二条　征信中心认为有关金融机构报送的信息可疑时，应按规定的程序及时向金融机构发出复核通知。

金融机构应当在收到复核通知之日起 5 个工作日内给予答复。

第三章　信用信息的查询

第十三条　金融机构在办理、管理信贷业务时，可以向企业信用数据库查询借款人、担保人信用信息。

第十四条　金融机构对申请信贷业务的借款人、担保人的信用信息进行查询时，要取得被查询人书面授权。

第十五条　金融机构对已发生信贷业务的借款人、担保人进行贷后风险管理查询其信用信息时，无须取得被查询人授权；当所有信贷业务关系解除后，金融机构不再具有对该借款人、担保人信用信息的查询权。

第十六条　金融机构应当制定查询借款人、担保人信用信息的内部授权制度和查询管理程序。

第十七条　金融机构通过查询企业信用数据库获取的借款人、担保人信用信息，不得用于本机构除办理、管理信贷业务之外的其他用途，不得向第三方提供。

第十八条　征信中心应当为符合法律、行政法规规定的单位和个人提供有关信息服务。

第十九条　征信中心可以根据借款人、担保人申请有偿提供其自身信用报告。

征信中心可以向取得借款人、担保人授权的单位和个人有偿提供其信用报告。

第四章　异议处理

第二十条　借款人、担保人认为自身信用报告中的信用信息不准确，可以通过中国人民银行分支机构或直接向征信中心提出书面异议申请。

第二十一条　征信中心应按中国人民银行发布的异议处理规程及有关要求对异议信息进行核查处理。经核查发现异议信息是由企业信用数据库信息处理过程造成的，征信中心应当及时更正，并检查企业信用数据库处理程序和操作规程存在的问题。

第二十二条　金融机构应按中国人民银行发布的异议处理规程及有关要求对异议信息进行核查处理，并应在 15 个工作日内对异议信息核查情况作出书面答复。

第二十三条　自受理异议信息之日起，征信中心应对该异议信息予以标注。

第二十四条　征信中心应在受理异议申请后 30 个工作日内，向提出异议申请的借款人、担保人提供书面答复，异议信息得到更正的，同时附更正后的信用报告。

异议信息确实有误，但因技术原因暂时无法更正异议信息的，征信中心应当在书面答复中予以说明，待异议信息更正后，提供更正后的信用报告。

第二十五条　对于无法核实的异议信息，征信中心应当允许提出异议申请的借款人、担保人对有关异议信息附注 200 字以内的声明。声明不得包含与异议信息无关的内容。提出异议申请的借款人、担保人应当对声明的真实性负责。

征信中心应当妥善保存声明原始档案，并将声明载入借款人、担保人信用报告。

第五章　安全管理

第二十六条　企业信用数据库的安全管理应符合国家有关计算机信息系统安全的法律法规规定。

第二十七条　金融机构应当建立用户管理制度，明确系统管理员用户、普通用户的职责及操作规程。

金融机构的系统管理员用户、普通用户不得互相兼职。

第二十八条　金融机构应将系统管理员用户和普通用户的名单及中国人民银行要求的相关资料报中国人民银行和征信中心备案。

前款用户发生变动，金融机构应当在 2 个工作日内向中国人民银行和征信中心变更备案。

第二十九条　征信中心及其工作人员不得违反法律、法规及本办法的规定，篡改、毁损、泄露或非法使用借款人、担保人信用信息，不得与自然人、法人、其他组织恶意串通，

提供虚假信用报告。

第三十条　征信中心应当建立企业信用数据库内部运行和外部访问的监控制度，监督企业信用数据库用户的操作，防范对企业信用数据库的非法入侵。

第三十一条　征信中心应当采取必要的安全保障措施保证系统安全，防止数据丢失。

第三十二条　征信中心应当对金融机构的所有查询进行记录，并及时向中国人民银行和金融机构反馈。

第六章　罚　则

第三十三条　金融机构未按照本办法制定相应管理制度的，由中国人民银行给予警告，责令其改正，并处以 3 万元罚款。

第三十四条　金融机构有下列行为之一的，由中国人民银行给予警告，责令其改正，逾期不改正的，处以 1 万元以上 3 万元以下的罚款；建议对该金融机构直接负责的主管人员和直接责任人给予纪律处分；涉嫌犯罪的，依法移交司法机关追究刑事责任：

（一）未准确、完整、及时报送借款人、担保人信用信息的；

（二）违反本办法第八条规定的；

（三）越权查询企业信用数据库的；

（四）将查询结果用于本机构办理和管理信贷业务之外的其他用途或向第三方提供的；

（五）违反异议处理规定的；

（六）违反本办法系统安全管理要求的；

（七）其他违反本办法的行为。

第三十五条　中国人民银行工作人员有下列情形之一的，依法给予行政处分；涉嫌犯罪的，依法移交司法机关追究刑事责任：

（一）泄露借款人、担保人信用信息的；

（二）其他违反本办法的行为。

第三十六条　征信中心工作人员有下列情形之一的，由中国人民银行依法给予行政处分；涉嫌犯罪的，依法移交司法机关追究刑事责任：

（一）违反本办法规定，篡改、毁损、泄露或非法使用借款人、担保人信用信息的；

（二）与自然人、法人、其他组织恶意串通，提供虚假信用报告的；

（三）违反本办法异议处理规定的；

（四）其他违反本办法的行为。

第七章　附　则

第三十七条　本办法所称借款人是指向金融机构办理信贷业务的法人、其他组织及个体工商户。担保人是指为借款人提供担保的法人、其他组织及自然人。

金融机构是指在中华人民共和国境内依法设立的政策性银行、商业银行（含外资银行）、城市信用社、农村信用社、金融资产管理公司、信托投资公司、财务公司、租赁公司以及经国务院金融监督管理机构批准的其他机构。

本办法所称借款人、担保人信用信息包括借款人、担保人的基本信息、信贷业务信息以及反映其信用状况的其他信息。

前款所称借款人、担保人基本信息是指借款人、担保人的概况信息及财务信息；信贷业务信息是指金融机构提供的借款人、担保人在贷款、担保、保理、票据贴现、信用证、保函、银行承兑汇票等信用活动中形成的交易记录；反映信用状况的其他信息是指除基本信息、信贷业务信息之外的反映借款人、担保人信用状况的其他相关信息。

第三十八条　公用事业组织和法律、行政法规规定的其他公共服务组织向企业信用数据库提供借款人、担保人信用信息的，以及尚未与金融机构发生信贷关系的法人、其他组织和个体工商户自愿向企业信用数据库提供自身信用信息的，参照本办法执行。

第三十九条　本办法由中国人民银行负责解释。

第四十条　本办法自　年　月　日起施行。

金融机构反洗钱规定

基本信息：

【发布机关】中国人民银行

【发文字号】中国人民银行令〔2006〕第1号

【发布日期】2006.11.14

【时效性】现行有效

【效力级别】部门规章

【实施日期】2007.01.01

金融机构反洗钱规定

第一条　为了预防洗钱活动，规范反洗钱监督管理行为和金融机构的反洗钱工作，维护金融秩序，根据《中华人民共和国反洗钱法》、《中华人民共和国中国人民银行法》等有关法律、行政法规，制定本规定。

第二条　本规定适用于在中华人民共和国境内依法设立的下列金融机构：

（一）商业银行、城市信用合作社、农村信用合作社、邮政储汇机构、政策性银行；

（二）证券公司、期货经纪公司、基金管理公司；

（三）保险公司、保险资产管理公司；

（四）信托投资公司、金融资产管理公司、财务公司、金融租赁公司、汽车金融公司、货币经纪公司；

（五）中国人民银行确定并公布的其他金融机构。

从事汇兑业务、支付清算业务和基金销售业务的机构适用本规定对金融机构反洗钱监督管理的规定。

第三条　中国人民银行是国务院反洗钱行政主管部门，依法对金融机构的反洗钱工作进行监督管理。中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会在各自的职责范围内履行反洗钱监督管理职责。

中国人民银行在履行反洗钱职责过程中，应当与国务院有关部门、机构和司法机关相互配合。

第四条　中国人民银行根据国务院授权代表中国政府开展反洗钱国际合作。中国人民银行可以和其他国家或者地区的反洗钱机构建立合作机制，实施跨境反洗钱监督管理。

第五条　中国人民银行依法履行下列反洗钱监督管理职责：

（一）制定或者会同中国银行业监督管理委员会、中国证券监督管理委员会和中国保险监督管理委员会制定金融机构反洗钱规章；

（二）负责人民币和外币反洗钱的资金监测；

（三）监督、检查金融机构履行反洗钱义务的情况；

（四）在职责范围内调查可疑交易活动；

（五）向侦查机关报告涉嫌洗钱犯罪的交易活动；

（六）按照有关法律、行政法规的规定，与境外反洗钱机构交换与反洗钱有关的信息和资料；

（七）国务院规定的其他有关职责。

第六条　中国人民银行设立中国反洗钱监测分析中心，依法履行下列职责：

（一）接收并分析人民币、外币大额交易和可疑交易报告；

（二）建立国家反洗钱数据库，妥善保存金融机构提交的大额交易和可疑交易报告信息；

（三）按照规定向中国人民银行报告分析结果；

（四）要求金融机构及时补正人民币、外币大额交易和可疑交易报告；

（五）经中国人民银行批准，与境外有关机构交换信息、资料；

（六）中国人民银行规定的其他职责。

第七条　中国人民银行及其工作人员应当对依法履行反洗钱职责获得的信息予以保密，不得违反规定对外提供。

中国反洗钱监测分析中心及其工作人员应当对依法履行反洗钱职责获得的客户身份资料、大额交易和可疑交易信息予以保密；非依法律规定，不得向任何单位和个人提供。

第八条　金融机构及其分支机构应当依法建立健全反洗钱内部控制制度，设立反洗钱专门机构或者指定内设机构负责反洗钱工作，制定反洗钱内部操作规程和控制措施，对工作人员进行反洗钱培训，增强反洗钱工作能力。

金融机构及其分支机构的负责人应当对反洗钱内部控制制度的有效实施负责。

第九条　金融机构应当按照规定建立和实施客户身份识别制度。

（一）对要求建立业务关系或者办理规定金额以上的一次性金融业务的客户身份进行识别，要求客户出示真实有效的身份证件或者其他身份证明文件，进行核对并登记，客户身份信息发生变化时，应当及时予以更新；

（二）按照规定了解客户的交易目的和交易性质，有效识别交易的受益人；

（三）在办理业务中发现异常迹象或者对先前获得的客户身份资料的真实性、有效性、完整性有疑问的，应当重新识别客户身份；

（四）保证与其有代理关系或者类似业务关系的境外金融机构进行有效的客户身份识别，并可从该境外金融机构获得所需的客户身份信息。

前款规定的具体实施办法由中国人民银行会同中国银行业监督管理委员会、中国证券监督管理委员会和中国保险监督管理委员会制定。

第十条　金融机构应当在规定的期限内，妥善保存客户身份资料和能够反映每笔交易的数据信息、业务凭证、账簿等相关资料。

前款规定的具体实施办法由中国人民银行会同中国银行业监督管理委员会、中国证券监督管理委员会、中国保险监督管理委员会制定。

第十一条　金融机构应当按照规定向中国反洗钱监测分析中心报告人民币、外币大额交易和可疑交易。

前款规定的具体实施办法由中国人民银行另行制定。

第十二条　中国人民银行会同中国银行业监督管理委员会、中国证券监督管理委员会、

中国保险监督管理委员会指导金融行业自律组织制定本行业的反洗钱工作指引。

第十三条　金融机构在履行反洗钱义务过程中，发现涉嫌犯罪的，应当及时以书面形式向中国人民银行当地分支机构和当地公安机关报告。

第十四条　金融机构及其工作人员应当依法协助、配合司法机关和行政执法机关打击洗钱活动。

金融机构的境外分支机构应当遵循驻在国家或者地区反洗钱方面的法律规定，协助配合驻在国家或者地区反洗钱机构的工作。

第十五条　金融机构及其工作人员对依法履行反洗钱义务获得的客户身份资料和交易信息应当予以保密；非依法律规定，不得向任何单位和个人提供。

金融机构及其工作人员应当对报告可疑交易、配合中国人民银行调查可疑交易活动等有关反洗钱工作信息予以保密，不得违反规定向客户和其他人员提供。

第十六条　金融机构及其工作人员依法提交大额交易和可疑交易报告，受法律保护。

第十七条　金融机构应当按照中国人民银行的规定，报送反洗钱统计报表、信息资料以及稽核审计报告中与反洗钱工作有关的内容。

第十八条　中国人民银行及其分支机构根据履行反洗钱职责的需要，可以采取下列措施进行反洗钱现场检查：

（一）进入金融机构进行检查；

（二）询问金融机构的工作人员，要求其对有关检查事项作出说明；

（三）查阅、复制金融机构与检查事项有关的文件、资料，并对可能被转移、销毁、隐匿或者篡改的文件资料予以封存；

（四）检查金融机构运用电子计算机管理业务数据的系统。

中国人民银行或者其分支机构实施现场检查前，应填写现场检查立项审批表，列明检查对象、检查内容、时间安排等内容，经中国人民银行或者其分支机构负责人批准后实施。

现场检查时，检查人员不得少于 2 人，并应出示执法证和检查通知书；检查人员少于 2 人或者未出示执法证和检查通知书的，金融机构有权拒绝检查。

现场检查后，中国人民银行或者其分支机构应当制作现场检查意见书，加盖公章，送达被检查机构。现场检查意见书的内容包括检查情况、检查评价、改进意见与措施。

第十九条　中国人民银行及其分支机构根据履行反洗钱职责的需要，可以与金融机构董事、高级管理人员谈话，要求其就金融机构履行反洗钱义务的重大事项作出说明。

第二十条　中国人民银行对金融机构实施现场检查，必要时将检查情况通报中国银行

业监督管理委员会、中国证券监督管理委员会或者中国保险监督管理委员会。

第二十一条　中国人民银行或者其省一级分支机构发现可疑交易活动需要调查核实的，可以向金融机构调查可疑交易活动涉及的客户账户信息、交易记录和其他有关资料，金融机构及其工作人员应当予以配合。

前款所称中国人民银行或者其省一级分支机构包括中国人民银行总行、上海总部、分行、营业管理部、省会（首府）城市中心支行、副省级城市中心支行。

第二十二条　中国人民银行或者其省一级分支机构调查可疑交易活动，可以询问金融机构的工作人员，要求其说明情况；查阅、复制被调查的金融机构客户的账户信息、交易记录和其他有关资料；对可能被转移、隐藏、篡改或者毁损的文件、资料，可以封存。

调查可疑交易活动时，调查人员不得少于 2 人，并出示执法证和中国人民银行或者其省一级分支机构出具的调查通知书。查阅、复制、封存被调查的金融机构客户的账户信息、交易记录和其他有关资料，应当经中国人民银行或者其省一级分支机构负责人批准。调查人员违反规定程序的，金融机构有权拒绝调查。

询问应当制作询问笔录。询问笔录应当交被询问人核对。记载有遗漏或者差错的，被询问人可以要求补充或者更正。被询问人确认笔录无误后，应当签名或者盖章；调查人员也应当在笔录上签名。

调查人员封存文件、资料，应当会同在场的金融机构工作人员查点清楚，当场开列清单一式二份，由调查人员和在场的金融机构工作人员签名或者盖章，一份交金融机构，一份附卷备查。

第二十三条　经调查仍不能排除洗钱嫌疑的，应当立即向有管辖权的侦查机关报案。对客户要求将调查所涉及的账户资金转往境外的，金融机构应当立即向中国人民银行当地分支机构报告。经中国人民银行负责人批准，中国人民银行可以采取临时冻结措施，并以书面形式通知金融机构，金融机构接到通知后应当立即予以执行。

侦查机关接到报案后，认为需要继续冻结的，金融机构在接到侦查机关继续冻结的通知后，应当予以配合。侦查机关认为不需要继续冻结的，中国人民银行在接到侦查机关不需要继续冻结的通知后，应当立即以书面形式通知金融机构解除临时冻结。

临时冻结不得超过 48 小时。金融机构在按照中国人民银行的要求采取临时冻结措施后 48 小时内，未接到侦查机关继续冻结通知的，应当立即解除临时冻结。

第二十四条　中国人民银行及其分支机构从事反洗钱工作的人员有下列行为之一的，依法给予行政处分：

（一）违反规定进行检查、调查或者采取临时冻结措施的；

（二）泄露因反洗钱知悉的国家秘密、商业秘密或者个人隐私的；

（三）违反规定对有关机构和人员实施行政处罚的；

（四）其他不依法履行职责的行为。

第二十五条　金融机构违反本规定的，由中国人民银行或者其地市中心支行以上分支机构按照《中华人民共和国反洗钱法》第三十一条、第三十二条的规定进行处罚；区别不同情形，建议中国银行业监督管理委员会、中国证券监督管理委员会或者中国保险监督管理委员会采取下列措施：

（一）责令金融机构停业整顿或者吊销其经营许可证；

（二）取消金融机构直接负责的董事、高级管理人员和其他直接责任人员的任职资格、禁止其从事有关金融行业工作；

（三）责令金融机构对直接负责的董事、高级管理人员和其他直接责任人员给予纪律处分。

中国人民银行县（市）支行发现金融机构违反本规定的，应报告其上一级分支机构，由该分支机构按照前款规定进行处罚或提出建议。

第二十六条　中国人民银行和其地市中心支行以上分支机构对金融机构违反本规定的行为给予行政处罚的，应当遵守《中国人民银行行政处罚程序规定》的有关规定。

第二十七条　本规定自 2007 年 1 月 1 日起施行。2003 年 1 月 3 日中国人民银行发布的《金融机构反洗钱规定》同时废止。

规范互联网信息服务市场秩序若干规定

基本信息：	
【发布机关】工业和信息化部	【时效性】 现行有效
【发文字号】中华人民共和国工业和信息化部令第 20 号	【效力级别】部门规章
【发布日期】2011.12.29	【实施日期】2012.03.15

规范互联网信息服务市场秩序若干规定【节选】

第十一条 未经用户同意，互联网信息服务提供者不得收集与用户相关、能够单独或者与其他信息结合识别用户的信息（以下简称“用户个人信息”），不得将用户个人信息提供给他人，但是法律、行政法规另有规定的除外。互联网信息服务提供者经用户同意收集用户个人信息的，应当明确告知用户收集和处理用户个人信息的方式、内容和用途，不得收

集其提供服务所必需以外的信息，不得将用户个人信息用于其提供服务之外的目的。

第十二条 互联网信息服务提供者应当妥善保管用户个人信息；保管的用户个人信息泄露或者可能泄露时，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予其互联网信息服务许可或者备案的电信管理机构报告，并配合相关部门进行的调查处理。

第十三条 互联网信息服务提供者应当加强系统安全防护，依法维护用户上载信息的安全，保障用户对上载信息的使用、修改和删除。互联网信息服务提供者不得有下列行为：（一）无正当理由擅自修改或者删除用户上载信息；（二）未经用户同意，向他人提供用户上载信息，但是法律、行政法规另有规定的除外；（三）擅自或者假借用户名义转移用户上载信息，或者欺骗、误导、强迫用户转移其上载信息；（四）其他危害用户上载信息安全的行为。

第十八条 互联网信息服务提供者违反本规定第八条、第九条、第十条、第十一条、第十二条或者第十四条的规定的，由电信管理机构依据职权处以警告，可以并处一万元以上三万元以下的罚款，向社会公告。

征信机构管理办法

基本信息：	
【发布机关】中国人民银行	【时效性】现行有效
【发文字号】中国人民银行令〔2013〕第1号	【效力级别】部门规章
【发布日期】2013.11.15	【实施日期】2013.12.20

征信机构管理办法

第一章　总 则

第一条　为加强对征信机构的监督管理，促进征信业健康发展，根据《中华人民共和国中国人民银行法》、《中华人民共和国公司法》、《征信业管理条例》等法律法规，制定本办法。

第二条　本办法所称征信机构，是指依法设立、主要经营征信业务的机构。

第三条　中国人民银行依法履行对征信机构的监督管理职责。中国人民银行分支机构在总行的授权范围内，履行对辖区内征信机构的监督管理职责。

第四条　征信机构应当遵守法律、行政法规和中国人民银行的规定，诚信经营，不得

损害国家利益、社会公共利益，不得侵犯他人合法权益。

第二章　机构的设立、变更与终止

第五条　设立个人征信机构应当经中国人民银行批准。

第六条　设立个人征信机构，除应当符合《征信业管理条例》第六条规定外，还应当具备以下条件：

（一）有健全的组织机构；

（二）有完善的业务操作、信息安全管理、合规性管理等内控制度；

（三）个人信用信息系统符合国家信息安全保护等级二级或二级以上标准。

《征信业管理条例》第六条第一项所称主要股东是指出资额占公司资本总额 5%以上或者持股占公司股份 5%以上的股东。

第七条　申请设立个人征信机构，应当向中国人民银行提交下列材料：

（一）个人征信机构设立申请表；

（二）征信业务可行性研究报告，包括发展规划、经营策略等；

（三）公司章程；

（四）股东关联关系和实际控制人说明；

（五）主要股东最近 3 年无重大违法违规行为的声明以及主要股东的信用报告；

（六）拟任董事、监事和高级管理人员任职资格证明；

（七）组织机构设置以及人员基本构成说明；

（八）已经建立的内控制度，包括业务操作、安全管理、合规性管理等；

（九）具有国家信息安全等级保护测评资质的机构出具的个人信用信息系统安全测评报告，关于信息安全保障措施的说明和相关安全保障制度；

（十）营业场所所有权或者使用权证明文件；

（十一）工商行政管理部门出具的企业名称预先核准通知书复印件。

中国人民银行可以通过实地调查、面谈等方式对申请材料进行核实。

第八条　中国人民银行在受理个人征信机构设立申请后公示申请人的下列事项：

（一）拟设立征信机构的名称、营业场所、业务范围；

（二）拟设立征信机构的资本；

（三）拟设立征信机构的主要股东名单及其出资额或者所持股份；

（四）拟任征信机构的董事、监事和高级管理人员名单。

第九条　中国人民银行自受理个人征信机构设立申请之日起 60 日内对申请事项进行审查，并根据有利于征信业公平竞争和健康发展的审慎性原则作出批准或者不予批准的决定。决定批准的，依法颁发个人征信业务经营许可证；决定不予批准的，应当作出书面决定。

第十条　经批准设立的个人征信机构，凭个人征信业务经营许可证向公司登记机关办理登记，领取营业执照；个人征信机构应当自公司登记机关准予登记之日起 20 日内，向中国人民银行提交营业执照复印件。

第十一条　个人征信机构拟合并或者分立的，应当向中国人民银行提出申请，说明申请和理由，并提交相关证明材料。

中国人民银行自受理申请之日起 20 日内，作出批准或者不予批准的书面决定。

第十二条　个人征信机构拟变更资本、主要股东的，应当向中国人民银行提出申请，说明变更事项和变更理由，并提交相关证明材料。

中国人民银行自受理申请之日起 20 日内，作出批准或者不予批准的书面决定。

第十三条　个人征信机构拟设立分支机构的，应当符合以下条件：

（一）对拟设立分支机构的可行性已经进行充分论证；

（二）最近 3 年无受到重大行政处罚的记录。

第十四条　个人征信机构申请设立分支机构，应当向中国人民银行提交下列材料：

（一）个人征信机构分支机构设立申请表；

（二）个人征信机构上一年度经审计的财务会计报告；

（三）设立分支机构的可行性论证报告，包括拟设立分支机构的 3 年业务发展规划、市场分析和经营方针等；

（四）针对设立分支机构所作出的内控制度安排和风险防范措施；

（五）个人征信机构最近 3 年未受重大行政处罚的声明；

（六）拟任职的分支机构高级管理人员履历材料。

中国人民银行自受理申请之日起 20 日内，作出批准或者不予批准的书面决定。

第十五条　个人征信机构变更机构名称、营业场所、法定代表人的，应当向中国人民银行申请变更个人征信业务经营许可证记载事项。

个人征信机构应当在个人征信业务经营许可证记载事项变更后，向公司登记机关申办

变更登记，并自公司登记机关准予变更之日起 20 日内，向中国人民银行备案。

第十六条　个人征信业务经营许可证应当在个人征信机构营业场所的显著位置公示。

第十七条　个人征信机构应当妥善保管个人征信业务经营许可证，不得涂改、倒卖、出租、出借、转让。

第十八条　个人征信业务经营许可证有效期为 3 年。有效期届满需要续展的，应当在有效期届满 60 日前向中国人民银行提出申请，换发个人征信业务经营许可证。

有效期届满不再续展的，个人征信机构应当在个人征信业务经营许可证有效期届满 60 日前向中国人民银行报告，并依照本办法第二十条的规定，妥善处理信息数据库，办理个人征信业务经营许可证注销手续；个人征信机构在个人征信业务经营许可证有效期届满 60 日前未提出续展申请的，中国人民银行可以在个人征信业务经营许可证有效期届满之日注销其个人征信业务经营许可证，并依照《征信业管理条例》第十二条的规定处理信息数据库。

第十九条　设立企业征信机构，应当符合《中华人民共和国公司法》规定的公司设立条件，自公司登记机关准予登记之日起 30 日内向所在地的中国人民银行省会（首府）城市中心支行以上分支机构办理备案，并提交下列材料：

（一）企业征信机构备案表；

（二）营业执照复印件；

（三）股权结构说明，包括资本、股东名单及其出资额或者所持股份；

（四）组织机构设置以及人员基本构成说明；

（五）业务范围和业务规则基本情况报告；

（六）业务系统的基本情况，包括企业信用信息系统建设情况报告和具有国家信息安全等级保护测评资质的机构出具的企业信用信息系统安全测评报告；

（七）信息安全和风险防范措施，包括已经建立的内控制度和安全管理制度。

企业征信机构备案事项发生变更的，应当自变更之日起 30 日内向备案机构办理变更备案。

第二十条　个人征信机构因解散或者被依法宣告破产等原因拟终止征信业务的，应当在拟终止之日前 60 日向中国人民银行报告退出方案，并依照《征信业管理条例》第十二条第一款规定处理信息数据库。

个人征信机构终止征信业务的，应当自终止之日起 20 日内，在中国人民银行指定的媒体上公告，并办理个人征信业务经营许可证注销手续，将许可证缴回中国人民银行；逾

期不缴回的，中国人民银行应当依法收缴。

第二十一条　企业征信机构因解散或者被依法宣告破产等原因拟终止征信业务的，应当在拟终止之日前 60 日向中国人民银行报告退出方案，并依照《征信业管理条例》第十二条第一款规定处理信息数据库。

第三章　高级任职人员管理

第二十二条　个人征信机构的董事、监事、高级管理人员，应当在任职前取得中国人民银行核准的任职资格。

第二十三条　取得个人征信机构董事、监事和高级管理人员任职资格，应当具备以下条件：

（一）正直诚实，品行良好；

（二）具有大专以上学历；

（三）从事征信工作 3 年以上或者从事金融、法律、会计、经济工作 5 年以上；

（四）具有履行职责所需的管理能力；

（五）熟悉与征信业务相关的法律法规和专业知识。

第二十四条　有下列情形之一的，不得担任个人征信机构董事、监事和高级管理人员：

（一）因贪污、贿赂、侵占财产、挪用财产或者破坏社会主义市场经济秩序，被判处刑罚，或者因犯罪被剥夺政治权利，执行期满未逾 5 年的；

（二）最近 3 年有重大违法违规记录的。

本办法所称重大违法违规记录，是指除前款第一项所列之外的犯罪记录或者重大行政处罚记录。

第二十五条　个人征信机构向中国人民银行申请核准董事、监事和高级管理人员的任职资格，应当提交下列材料：

（一）董事、监事和高级管理人员任职资格申请表；

（二）拟任职的董事、监事和高级管理人员的个人履历材料；

（三）拟任职的董事、监事和高级管理人员的学历证书复印件；

（四）拟任职的董事、监事和高级管理人员最近 3 年无重大违法违规记录的声明；

（五）拟任职的董事、监事和高级管理人员的个人信用报告。

个人征信机构应当如实提交前款规定的材料，个人征信机构以及拟任职的董事、监事和高级管理人员应当对材料的真实性、完整性负责。中国人民银行根据需要对材料的真实

性进行核实，并对申请任职资格的董事、监事和高级管理人员进行考察或者谈话。

第二十六条　中国人民银行依法对个人征信机构董事、监事和高级管理人员的任职资格进行审查，作出核准或者不予核准的书面决定。

第二十七条　企业征信机构的董事、监事、高级管理人员，应当由任职的征信机构自任命之日起 20 日内向所在地的中国人民银行省会（首府）城市中心支行以上分支机构备案，并提交下列材料：

（一）董事、监事、高级管理人员备案表；

（二）董事、监事、高级管理人员的个人履历材料；

（三）董事、监事、高级管理人员的学历证书复印件；

（四）董事、监事、高级管理人员的备案材料真实性声明。

企业征信机构的董事、监事、高级管理人员发生变更的，应当自变更之日起 20 日内向备案机构办理变更备案。

第四章　监督管理

第二十八条　个人征信机构应当在每年第一季度末，向中国人民银行报告上一年度征信业务开展情况。

企业征信机构应当在每年第一季度末，向备案机构报告上一年度征信业务开展情况。

报告内容应当包括信用信息采集、征信产品开发、信用信息服务、异议处理以及信用信息系统建设情况，信息安全保障情况等。

第二十九条　个人征信机构应当按规定向中国人民银行报送征信业务统计报表、财务会计报告、审计报告等资料。

企业征信机构应当按规定向备案机构报送征信业务统计报表、财务会计报告、审计报告等资料。

征信机构应当对报送的报表和资料的真实性、准确性、完整性负责。

第三十条　征信机构应当按照国家信息安全保护等级测评标准，对信用信息系统的安全情况进行测评。

征信机构信用信息系统安全保护等级为二级的，应当每两年进行测评；信用信息系统安全保护等级为三级以及以上的，应当每年进行测评。

个人征信机构应当自具有国家信息安全等级保护测评资质的机构出具测评报告之日起 20 日内，将测评报告报送中国人民银行，企业征信机构应当将测评报告报送备案机构。

第三十一条　征信机构有下列情形之一的，中国人民银行及其分支机构可以将其列为重点监管对象：

（一）上一年度发生严重违法违规行为的；

（二）出现可能发生信息泄露征兆的；

（三）出现财务状况异常或者严重亏损的；

（四）被大量投诉的；

（五）未按本办法第二十八条、第二十九条、第三十条规定报送相关材料的；

（六）中国人民银行认为需要重点监管的其他情形。

征信机构被列为重点监管对象的，中国人民银行及其分支机构可以酌情缩短征信机构报告征信业务开展情况、进行信用信息系统安全情况测评的周期，并采取相应的监管措施，督促征信机构整改。

整改后第一款中所列情形消除的，中国人民银行及其分支机构可不再将其列为重点监管对象。

第三十二条　中国人民银行及其分支机构可以根据监管需要，约谈征信机构董事、监事和高级管理人员，要求其就征信业务经营、风险控制、内部管理等有关重大事项作出说明。

第五章　罚 则

第三十三条　申请设立个人征信机构的申请人隐瞒有关情况或者提供虚假材料的，中国人民银行依照《中华人民共和国行政许可法》的相关规定进行处罚。

第三十四条　个人征信机构的个人信用信息系统未达到国家信息安全保护等级二级或者二级以上要求的，中国人民银行可以责令整顿；情节严重或者拒不整顿的，中国人民银行依照《征信业管理条例》第三十八条的规定，吊销其个人征信业务经营许可证。

第三十五条　申请个人征信机构的董事、监事、高级管理人员任职资格的申请人隐瞒有关情况或者提供虚假材料的，中国人民银行不予受理或者不予核准其任职资格，并给予警告；已经核准的，取消其任职资格。

禁止上述申请人 3 年内再次申请任职资格。

第三十六条　个人征信机构任命未取得任职资格董事、监事、高级管理人员的，由中国人民银行责令改正并给予警告；情节严重的，处 1 万元以上 3 万元以下罚款。

企业征信机构任命董事、监事、高级管理人员未及时备案或者变更备案，以及在备案中提供虚假材料的，由中国人民银行分支机构责令改正并给予警告；情节严重的，处 1 万

元以上 3 万元以下罚款。

第三十七条　征信机构违反本办法第二十九条、第三十条规定的，由中国人民银行及其分支机构责令改正；情节严重的，处 1 万元以上 3 万元以下罚款；涉嫌犯罪的，依法移交司法机关追究其刑事责任。

第六章　附 则

第三十八条　本办法由中国人民银行负责解释。

第三十九条　本办法自 2013 年 12 月 20 日起施行。

网络交易管理办法

基本信息：	
【发布机关】国家工商行政管理总局(已撤销)	【时效性】 现行有效
【发文字号】中华人民共和国国家工商行政管理总局令第 60 号	【效力级别】部门规章
【发布日期】2014.01.26	【实施日期】2014.03.15

网络交易管理办法【节选】

网络商品经营者和有关服务经营者的义务

第一节 一般性规定

第十八条 网络商品经营者、有关服务经营者在经营活动中收集、使用消费者或者经营者信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络商品经营者、有关服务经营者收集、使用消费者或者经营者信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。网络商品经营者、有关服务经营者及其工作人员对收集的消费者个人信息或者经营者商业秘密的数据信息必须严格保密，不得泄露、出售或者非法向他人提供。网络商品经营者、有关服务经营者应当采取技术措施和其他必要措施，确保信息安全，防止信息泄露、丢失。在发生或者可能发生信息泄露、丢失的情况时，应当立即采取补救措施。 网络商品经营者、有关服务经营者未经消费者同意或者请求，或者消费者明确表示拒绝的，不得向其发送商业性电子信息。

第二节　第三方交易平台经营者的特别规定

第二十三条 第三方交易平台经营者应当对申请进入平台销售商品或者提供服务的法人、其他经济组织或者个体工商户的经营主体身份进行审查和登记，建立登记档案并定期核实

更新，在其从事经营活动的主页面醒目位置公开营业执照登载的信息或者其营业执照的电子链接标识。 第三方交易平台经营者应当对尚不具备工商登记注册条件、申请进入平台销售商品或者提供服务的自然人的真实身份信息进行审查和登记，建立登记档案并定期核实更新，核发证明个人身份信息真实合法的标记，加载在其从事经营活动的主页面醒目位置。第三方交易平台经营者在审查和登记时，应当使对方知悉并同意登记协议，提请对方注意义务和责任条款。

第三十条 第三方交易平台经营者应当审查、记录、保存在其平台上发布的商品和服务信息内容及其发布时间。平台内经营者的营业执照或者个人真实身份信息记录保存时间从经营者在平台的登记注销之日起不少于两年，交易记录等其他信息记录备份保存时间从交易完成之日起不少于两年。 第三方交易平台经营者应当采取电子签名、数据备份、故障恢复等技术手段确保网络交易数据和资料的完整性和安全性，并应当保证原始数据的真实性。

第三节　其他有关服务经营者的特别规定

第三十五条 为网络商品交易提供网络接入、服务器托管、虚拟空间租用、网站网页设计制作等服务的有关服务经营者，应当要求申请者提供经营资格证明和个人真实身份信息，签订服务合同，依法记录其上网信息。申请者营业执照或者个人真实身份信息等信息记录备份保存时间自服务合同终止或者履行完毕之日起不少于两年。

第三十六条 为网络商品交易提供信用评价服务的有关服务经营者，应当通过合法途径采集信用信息，坚持中立、公正、客观原则，不得任意调整用户的信用级别或者相关信息，不得将收集的信用信息用于任何非法用途。

第四章　法律责任

第四十九条　对于违反本办法的行为，法律、法规另有规定的，从其规定。

第五十条　违反本办法第七条第二款、第二十三条、第二十五条、第二十六条第二款、第二十九条、第三十条、第三十四条、第三十五条、第三十六条、第三十八条规定的，予以警告，责令改正，拒不改正的，处以一万元以上三万元以下的罚款。

网络借贷信息中介机构业务活动管理暂行办法

基本信息：

【发布机关】中国银行业监督管理委员会(已撤销)，工业和信息化部，公安部，国家互联网信息办公室

【发文字号】中国银行业监督管理委员会、中华

【时效性】 现行有效

【发布日期】2016.08.17

【效力级别】部门规章

人民共和国工业和信息化部、中华人民共和国公安部、国家互联网信息办公室令 2016 年第 1 号	【实施日期】2016.08.17

网络借贷信息中介机构业务活动管理暂行办法【节选】

第三章　业务规则与风险管理

第十二条 借款人应当履行下列义务：

（一）提供真实、准确、完整的用户信息及融资信息；

（二）提供在所有网络借贷信息中介机构未偿还借款信息；

（三）保证融资项目真实、合法，并按照约定用途使用借贷资金，不得用于出借等其他目的；

（四）按照约定向出借人如实报告影响或可能影响出借人权益的重大信息；

（五）确保自身具有与借款金额相匹配的还款能力并按照合同约定还款；

（六）借贷合同及有关协议约定的其他义务。

第十五条 参与网络借贷的出借人应当履行下列义务：

（一）向网络借贷信息中介机构提供真实、准确、完整的身份等信息；

（二）出借资金为来源合法的自有资金；

（三）了解融资项目信贷风险，确认具有相应的风险认知和承受能力；

（四）自行承担借贷产生的本息损失；

（五）借贷合同及有关协议约定的其他义务。

第十八条 网络借贷信息中介机构应当按照国家网络安全相关规定和国家信息安全等级保护制度的要求，开展信息系统定级备案和等级测试，具有完善的防火墙、入侵检测、数据加密以及灾难恢复等网络安全设施和管理制度，建立信息科技管理、科技风险管理和科技审计有关制度，配置充足的资源，采取完善的管理控制措施和技术手段保障信息系统安全稳健运行，保护出借人与借款人的信息安全。网络借贷信息中介机构应当记录并留存借贷双方上网日志信息，信息交互内容等数据，留存期限为自借贷合同到期起 5 年；每两年至少开展一次全面的安全评估，接受国家或行业主管部门的信息安全检查和审计。网络借贷信息中介机构成立两年以内，应当建立或使用与其业务规模相匹配的应用级灾备系统设施。

第四章　出借人与借款人保护

第二十七条 网络借贷信息中介机构应当加强出借人与借款人信息管理，确保出借人与

借款人信息采集、处理及使用的合法性和安全性。网络借贷信息中介机构及其资金存管机构、其他各类外包服务机构等应当为业务开展过程中收集的出借人与借款人信息保密，未经出借人与借款人同意，不得将出借人与借款人提供的信息用于所提供服务之外的目的。在中国境内收集的出借人与借款人信息的储存、处理和分析应当在中国境内进行。除法律法规另有规定外，网络借贷信息中介机构不得向境外提供境内出借人和借款人信息。

第五章　信息披露

第三十条 网络借贷信息中介机构应当在其官方网站上向出借人充分披露借款人基本信息、融资项目基本信息、风险评估及可能产生的风险结果、已撮合未到期融资项目资金运用情况等有关信息。 披露内容应符合法律法规关于国家秘密、商业秘密、个人隐私的有关规定。

第三十二条 网络借贷信息中介机构的董事、监事、高级管理人员应当忠实、勤勉地履行职责，保证披露的信息真实、准确、完整、及时、公平，不得有虚假记载、误导性陈述或者重大遗漏。 借款人应当配合网络借贷信息中介机构及出借人对融资项目有关信息的调查核实，保证提供的信息真实、准确、完整。网络借贷信息披露具体细则另行制定。

金融机构大额交易和可疑交易报告管理办法（2016 修订）

基本信息：	
【发布机关】中国人民银行	【时效性】现行有效
【发文字号】中国人民银行令〔2016〕第 3 号	【效力级别】部门规章
【发布日期】2016.12.28	【实施日期】2017.07.01

金融机构大额交易和可疑交易报告管理办法(2016 修订)

第一章 总　则

第一条　为了规范金融机构大额交易和可疑交易报告行为，根据《中华人民共和国反洗钱法》、《中华人民共和国中国人民银行法》、《中华人民共和国反恐怖主义法》等有关法律法规，制定本办法。

第二条　本办法适用于在中华人民共和国境内依法设立的下列金融机构：

（一）政策性银行、商业银行、农村合作银行、农村信用社、村镇银行。

（二）证券公司、期货公司、基金管理公司。

（三）保险公司、保险资产管理公司、保险专业代理公司、保险经纪公司。

（四）信托公司、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、贷款公司。

（五）中国人民银行确定并公布的应当履行反洗钱义务的从事金融业务的其他机构。

第三条　金融机构应当履行大额交易和可疑交易报告义务，向中国反洗钱监测分析中心报送大额交易和可疑交易报告，接受中国人民银行及其分支机构的监督、检查。

第四条　金融机构应当通过其总部或者总部指定的一个机构，按本办法规定的路径和方式提交大额交易和可疑交易报告。

第二章 大额交易报告

第五条　金融机构应当报告下列大额交易：

（一）当日单笔或者累计交易人民币 5 万元以上（含 5 万元）、外币等值 1 万美元以上（含 1 万美元）的现金缴存、现金支取、现金结售汇、现钞兑换、现金汇款、现金票据解付及其他形式的现金收支。

（二）非自然人客户银行账户与其他的银行账户发生当日单笔或者累计交易人民币 200 万元以上（含 200 万元）、外币等值 20 万美元以上（含 20 万美元）的款项划转。

（三）自然人客户银行账户与其他的银行账户发生当日单笔或者累计交易人民币 50 万元以上（含 50 万元）、外币等值 10 万美元以上（含 10 万美元）的境内款项划转。

（四）自然人客户银行账户与其他的银行账户发生当日单笔或者累计交易人民币 20 万元以上（含 20 万元）、外币等值 1 万美元以上（含 1 万美元）的跨境款项划转。

累计交易金额以客户为单位，按资金收入或者支出单边累计计算并报告。中国人民银行另有规定的除外。

中国人民银行根据需要可以调整本条第一款规定的大额交易报告标准。

第六条　对同时符合两项以上大额交易标准的交易，金融机构应当分别提交大额交易报告。

第七条　对符合下列条件之一的大额交易，如未发现交易或行为可疑的，金融机构可以不报告：

（一）定期存款到期后，不直接提取或者划转，而是本金或者本金加全部或者部分利息续存入在同一金融机构开立的同一户名下的另一账户。

活期存款的本金或者本金加全部或者部分利息转为在同一金融机构开立的同一户名下的另一账户内的定期存款。

定期存款的本金或者本金加全部或者部分利息转为在同一金融机构开立的同一户名下

的另一账户内的活期存款。

（二）自然人实盘外汇买卖交易过程中不同外币币种间的转换。

（三）交易一方为各级党的机关、国家权力机关、行政机关、司法机关、军事机关、人民政协机关和人民解放军、武警部队，但不包含其下属的各类企事业单位。

（四）金融机构同业拆借、在银行间债券市场进行的债券交易。

（五）金融机构在黄金交易所进行的黄金交易。

（六）金融机构内部调拨资金。

（七）国际金融组织和外国政府贷款转贷业务项下的交易。

（八）国际金融组织和外国政府贷款项下的债务掉期交易。

（九）政策性银行、商业银行、农村合作银行、农村信用社、村镇银行办理的税收、错账冲正、利息支付。

（十）中国人民银行确定的其他情形。

第八条　金融机构应当在大额交易发生之日起 5 个工作日内以电子方式提交大额交易报告。

第九条　下列金融机构与客户进行金融交易并通过银行账户划转款项的，由银行机构按照本办法规定提交大额交易报告：

（一）证券公司、期货公司、基金管理公司。

（二）保险公司、保险资产管理公司、保险专业代理公司、保险经纪公司。

（三）信托公司、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、贷款公司。

第十条　客户通过在境内金融机构开立的账户或者境内银行卡所发生的大额交易，由开立账户的金融机构或者发卡银行报告；客户通过境外银行卡所发生的大额交易，由收单机构报告；客户不通过账户或者银行卡发生的大额交易，由办理业务的金融机构报告。

第三章 可疑交易报告

第十一条　金融机构发现或者有合理理由怀疑客户、客户的资金或者其他资产、客户的交易或者试图进行的交易与洗钱、恐怖融资等犯罪活动相关的，不论所涉资金金额或者资产价值大小，应当提交可疑交易报告。

第十二条　金融机构应当制定本机构的交易监测标准，并对其有效性负责。交易监测标准包括并不限于客户的身份、行为，交易的资金来源、金额、频率、流向、性质等存在

异常的情形，并应当参考以下因素：

（一）中国人民银行及其分支机构发布的反洗钱、反恐怖融资规定及指引、风险提示、洗钱类型分析报告和风险评估报告。

（二）公安机关、司法机关发布的犯罪形势分析、风险提示、犯罪类型报告和工作报告。

（三）本机构的资产规模、地域分布、业务特点、客户群体、交易特征，洗钱和恐怖融资风险评估结论。

（四）中国人民银行及其分支机构出具的反洗钱监管意见。

（五）中国人民银行要求关注的其他因素。

第十三条　金融机构应当定期对交易监测标准进行评估，并根据评估结果完善交易监测标准。如发生突发情况或者应当关注的情况的，金融机构应当及时评估和完善交易监测标准。

第十四条　金融机构应当对通过交易监测标准筛选出的交易进行人工分析、识别，并记录分析过程；不作为可疑交易报告的，应当记录分析排除的合理理由；确认为可疑交易的，应当在可疑交易报告理由中完整记录对客户身份特征、交易特征或行为特征的分析过程。

第十五条　金融机构应当在按本机构可疑交易报告内部操作规程确认为可疑交易后，及时以电子方式提交可疑交易报告，最迟不超过 5 个工作日。

第十六条　既属于大额交易又属于可疑交易的交易，金融机构应当分别提交大额交易报告和可疑交易报告。

第十七条　可疑交易符合下列情形之一的，金融机构应当在向中国反洗钱监测分析中心提交可疑交易报告的同时，以电子形式或书面形式向所在地中国人民银行或者其分支机构报告，并配合反洗钱调查：

（一）明显涉嫌洗钱、恐怖融资等犯罪活动的。

（二）严重危害国家安全或者影响社会稳定的。

（三）其他情节严重或者情况紧急的情形。

第十八条　金融机构应当对下列恐怖活动组织及恐怖活动人员名单开展实时监测，有合理理由怀疑客户或者其交易对手、资金或者其他资产与名单相关的，应当在立即向中国反洗钱监测分析中心提交可疑交易报告的同时，以电子形式或书面形式向所在地中国人民银行或者其分支机构报告，并按照相关主管部门的要求依法采取措施。

（一）中国政府发布的或者要求执行的恐怖活动组织及恐怖活动人员名单。

（二）联合国安理会决议中所列的恐怖活动组织及恐怖活动人员名单。

（三）中国人民银行要求关注的其他涉嫌恐怖活动的组织及人员名单。

恐怖活动组织及恐怖活动人员名单调整的，金融机构应当立即开展回溯性调查，并按前款规定提交可疑交易报告。

法律、行政法规、规章对上述名单的监控另有规定的，从其规定。

第四章 内部管理措施

第十九条　金融机构应当根据本办法制定大额交易和可疑交易报告内部管理制度和操作规程，对本机构的大额交易和可疑交易报告工作做出统一要求，并对分支机构、附属机构大额交易和可疑交易报告制度的执行情况进行监督管理。

金融机构应当将大额交易和可疑交易报告制度向中国人民银行或其总部所在地的中国人民银行分支机构报备。

第二十条　金融机构应当设立专职的反洗钱岗位，配备专职人员负责大额交易和可疑交易报告工作，并提供必要的资源保障和信息支持。

第二十一条　金融机构应当建立健全大额交易和可疑交易监测系统，以客户为基本单位开展资金交易的监测分析，全面、完整、准确地采集各业务系统的客户身份信息和交易信息，保障大额交易和可疑交易监测分析的数据需求。

第二十二条　金融机构应当按照完整准确、安全保密的原则，将大额交易和可疑交易报告、反映交易分析和内部处理情况的工作记录等资料自生成之日起至少保存 5 年。

保存的信息资料涉及正在被反洗钱调查的可疑交易活动，且反洗钱调查工作在前款规定的最低保存期届满时仍未结束的，金融机构应将其保存至反洗钱调查工作结束。

第二十三条　金融机构及其工作人员应当对依法履行大额交易和可疑交易报告义务获得的客户身份资料和交易信息，对依法监测、分析、报告可疑交易的有关情况予以保密，不得违反规定向任何单位和个人提供。

第五章 法律责任

第二十四条　金融机构违反本办法的，由中国人民银行或者其地市中心支行以上分支机构按照《中华人民共和国反洗钱法》第三十一条、第三十二条的规定予以处罚。

第六章 附　则

第二十五条　非银行支付机构、从事汇兑业务和基金销售业务的机构报告大额交易和可疑交易适用本办法。银行卡清算机构、资金清算中心等从事清算业务的机构应当按照中

国人民银行有关规定开展交易监测分析、报告工作。

本办法所称非银行支付机构，是指根据《非金融机构支付服务管理办法》（中国人民银行令〔2010〕第 2 号发布）规定取得《支付业务许可证》的支付机构。

本办法所称资金清算中心，包括城市商业银行资金清算中心、农信银资金清算中心有限责任公司及中国人民银行确定的其他资金清算中心。

第二十六条　本办法所称非自然人，包括法人、其他组织和个体工商户。

第二十七条　金融机构应当按照本办法所附的大额交易和可疑交易报告要素要求（要素内容见附件），制作大额交易报告和可疑交易报告的电子文件。具体的报告格式和填报要求由中国人民银行另行规定。

第二十八条　中国反洗钱监测分析中心发现金融机构报送的大额交易报告或者可疑交易报告内容要素不全或者存在错误的，可以向提交报告的金融机构发出补正通知，金融机构应当在接到补正通知之日起 5 个工作日内补正。

第二十九条　本办法由中国人民银行负责解释。

第三十条　本办法自 2017 年 7 月 1 日起施行。中国人民银行 2006 年 11 月 14 日发布的《金融机构大额交易和可疑交易报告管理办法》（中国人民银行令〔2006〕第 2 号）和 2007 年 6 月 11 日发布的《金融机构报告涉嫌恐怖融资的可疑交易管理办法》（中国人民银行令〔2007〕第 1 号）同时废止。中国人民银行此前发布的大额交易和可疑交易报告的其他规定，与本办法不一致的，以本办法为准。

银行业金融机构反洗钱和反恐怖融资管理办法

基本信息：	
【发布机关】中国银行保险监督管理委员会	【时效性】现行有效 【效力级别】部门规章
【发文字号】中国银保监会令〔2019〕第 1 号	【实施日期】2019.01.29
【发布日期】2019.01.29	

银行业金融机构反洗钱和反恐怖融资管理办法

第一章　总　则

第一条　为预防洗钱和恐怖融资活动，做好银行业金融机构反洗钱和反恐怖融资工作，根据《中华人民共和国银行业监督管理法》《中华人民共和国反洗钱法》《中华人民共和

国反恐怖主义法》等有关法律、行政法规，制定本办法。

第二条　国务院银行业监督管理机构根据法律、行政法规规定，配合国务院反洗钱行政主管部门，履行银行业金融机构反洗钱和反恐怖融资监督管理职责。

国务院银行业监督管理机构的派出机构根据法律、行政法规及本办法的规定，负责辖内银行业金融机构反洗钱和反恐怖融资监督管理工作。

第三条　本办法所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、农村合作银行、农村信用合作社等吸收公众存款的金融机构以及政策性银行和国家开发银行。

对在中华人民共和国境内设立的金融资产管理公司、信托公司、企业集团财务公司、金融租赁公司、汽车金融公司、货币经纪公司、消费金融公司以及经国务院银行业监督管理机构批准设立的其他金融机构的反洗钱和反恐怖融资管理，参照本办法对银行业金融机构的规定执行。

第四条　银行业金融机构境外分支机构和附属机构，应当遵循驻在国家（地区）反洗钱和反恐怖融资方面的法律规定，协助配合驻在国家（地区）监管机构的工作，同时在驻在国家（地区）法律规定允许的范围内，执行本办法的有关要求。

驻在国家（地区）不允许执行本办法的有关要求的，银行业金融机构应当采取适当的额外措施应对洗钱和恐怖融资风险，并向国务院银行业监督管理机构报告。

第二章　银行业金融机构反洗钱和反恐怖融资义务

第五条　银行业金融机构应当建立健全洗钱和恐怖融资风险管理体系，全面识别和评估自身面临的洗钱和恐怖融资风险，采取与风险相适应的政策和程序。

第六条　银行业金融机构应当将洗钱和恐怖融资风险管理纳入全面风险管理体系，将反洗钱和反恐怖融资要求嵌入合规管理、内部控制制度，确保洗钱和恐怖融资风险管理体系能够全面覆盖各项产品及服务。

第七条　银行业金融机构应当依法建立反洗钱和反恐怖融资内部控制制度，并对分支机构和附属机构的执行情况进行管理。反洗钱和反恐怖融资内部控制制度应当包括下列内容：

（一）反洗钱和反恐怖融资内部控制职责划分；

（二）反洗钱和反恐怖融资内部控制措施；

（三）反洗钱和反恐怖融资内部控制评价机制；

（四）反洗钱和反恐怖融资内部控制监督制度；

（五）重大洗钱和恐怖融资风险事件应急处置机制；

（六）反洗钱和反恐怖融资工作信息保密制度；

（七）国务院银行业监督管理机构及国务院反洗钱行政主管部门规定的其他内容。

第八条　银行业金融机构应当建立组织架构健全、职责边界清晰的洗钱和恐怖融资风险治理架构，明确董事会、监事会、高级管理层、业务部门、反洗钱和反恐怖融资管理部门和内审部门等在洗钱和恐怖融资风险管理中的职责分工。

第九条　银行业金融机构董事会应当对反洗钱和反恐怖融资工作承担最终责任。

第十条　银行业金融机构的高级管理层应当承担洗钱和恐怖融资风险管理的实施责任。

银行业金融机构应当任命或者授权一名高级管理人员牵头负责洗钱和恐怖融资风险管理工作，其有权独立开展工作。银行业金融机构应当确保其能够充分获取履职所需的权限和资源，避免可能影响其履职的利益冲突。

第十一条　银行业金融机构应当设立反洗钱和反恐怖融资专门机构或者指定内设机构负责反洗钱和反恐怖融资管理工作。反洗钱和反恐怖融资管理部门应当设立专门的反洗钱和反恐怖融资岗位，并配备足够人员。

银行业金融机构应当明确相关业务部门的反洗钱和反恐怖融资职责，保证反洗钱和反恐怖融资内部控制制度在业务流程中的贯彻执行。

第十二条　银行业金融机构应当按照规定建立健全和执行客户身份识别制度，遵循“了解你的客户”的原则，针对不同客户、业务关系或者交易，采取有效措施，识别和核实客户身份，了解客户及其建立、维持业务关系的目的和性质，了解非自然人客户受益所有人。在与客户的业务关系存续期间，银行业金融机构应当采取持续的客户身份识别措施。

第十三条　银行业金融机构应当按照规定建立健全和执行客户身份资料和交易记录保存制度，妥善保存客户身份资料和交易记录，确保能重现该项交易，以提供监测分析交易情况、调查可疑交易活动和查处洗钱案件所需的信息。

第十四条　银行业金融机构应当按照规定建立健全和执行大额交易和可疑交易报告制度。

第十五条　银行业金融机构与金融机构开展业务合作时，应当在合作协议中明确双方的反洗钱和反恐怖融资职责，承担相应的法律义务，相互间提供必要的协助，采取有效的风险管控措施。

第十六条　银行业金融机构解散、撤销或者破产时，应当将客户身份资料和交易记录移交国务院有关部门指定的机构。

第十七条　银行业金融机构应当按照客户特点或者账户属性，以客户为单位合理确定洗钱和恐怖融资风险等级，根据风险状况采取相应的控制措施，并在持续关注的基础上适时调整风险等级。

第十八条　银行业金融机构应当建立健全和执行洗钱和恐怖融资风险自评估制度，对本机构的内外部洗钱和恐怖融资风险及相关风险控制措施有效性进行评估。

银行业金融机构开展新业务、应用新技术之前应当进行洗钱和恐怖融资风险评估。

第十九条　银行业金融机构应当建立反恐怖融资管理机制，按照国家反恐怖主义工作领导机构发布的恐怖活动组织及恐怖活动人员名单、冻结资产的决定，依法对相关资产采取冻结措施。

银行业金融机构应当根据监管要求密切关注涉恐人员名单，及时对本机构客户和交易进行风险排查，依法采取相应措施。

第二十条　银行业金融机构应当依法执行联合国安理会制裁决议要求。

第二十一条　银行业金融机构应当每年开展反洗钱和反恐怖融资内部审计，内部审计可以是专项审计，或者与其他审计项目结合进行。

第二十二条　对依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息，银行业金融机构及其工作人员应当予以保密；非依法律规定，不得向任何单位和个人提供。

第二十三条　银行业金融机构应当将可量化的反洗钱和反恐怖融资控制指标嵌入信息系统，使风险信息能够在业务部门和反洗钱和反恐怖融资管理部门之间有效传递、集中和共享，满足对洗钱和恐怖融资风险进行预警、信息提取、分析和报告等各项要求。

第二十四条　银行业金融机构应当配合银行业监督管理机构做好反洗钱和反恐怖融资监督检查工作。

第二十五条　银行业金融机构应当按照法律、行政法规及银行业监督管理机构的相关规定，履行协助查询、冻结、扣划义务，配合公安机关、司法机关等做好洗钱和恐怖融资案件调查工作。

第二十六条　银行业金融机构应当做好境外洗钱和恐怖融资风险管控和合规经营工作。境外分支机构和附属机构要加强与境外监管当局的沟通，严格遵守境外反洗钱和反恐怖融资法律法规及相关监管要求。

银行业金融机构境外分支机构和附属机构受到当地监管部门或者司法部门现场检查、行政处罚、刑事调查或者发生其他重大风险事项时，应当及时向银行业监督管理机构报告。

第二十七条　银行业金融机构应当对跨境业务开展尽职调查和交易监测工作，做好跨

境业务洗钱风险、制裁风险和恐怖融资风险防控，严格落实代理行尽职调查与风险分类评级义务。

第二十八条　对依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息，非依法律、行政法规规定，银行业金融机构不得向境外提供。

银行业金融机构对于涉及跨境信息提供的相关问题应当及时向银行业监督管理机构报告，并按照法律法规要求采取相应措施。

第二十九条　银行业金融机构应当制定反洗钱和反恐怖融资培训制度，定期开展反洗钱和反恐怖融资培训。

第三十条　银行业金融机构应当开展反洗钱和反恐怖融资宣传，保存宣传资料和宣传工作记录。

第三章　监督管理

第三十一条　国务院银行业监督管理机构依法履行下列反洗钱和反恐怖融资监督管理职责：

（一）制定银行业金融机构反洗钱和反恐怖融资制度文件；

（二）督促指导银行业金融机构建立健全反洗钱和反恐怖融资内部控制制度；

（三）监督、检查银行业金融机构反洗钱和反恐怖融资内部控制制度建立执行情况；

（四）在市场准入工作中落实反洗钱和反恐怖融资审查要求；

（五）与其他国家或者地区的银行业监督管理机构开展反洗钱和反恐怖融资监管合作；

（六）指导银行业金融机构依法履行协助查询、冻结、扣划义务；

（七）转发联合国安理会相关制裁决议，依法督促银行业金融机构落实金融制裁要求；

（八）向侦查机关报送涉嫌洗钱和恐怖融资犯罪的交易活动，协助公安机关、司法机关等调查处理涉嫌洗钱和恐怖融资犯罪案件；

（九）指导银行业金融机构应对境外协助执行案件、跨境信息提供等相关工作；

（十）指导行业自律组织开展反洗钱和反恐怖融资工作；

（十一）组织开展反洗钱和反恐怖融资培训宣传工作；

（十二）其他依法应当履行的反洗钱和反恐怖融资职责。

第三十二条　银行业监督管理机构应当履行银行业反洗钱和反恐怖融资监管职责，加强反洗钱和反恐怖融资日常合规监管，构建涵盖事前、事中、事后的完整监管链条。

银行业监督管理机构与国务院反洗钱行政主管部门及其他相关部门要加强监管协调，

建立信息共享机制。

第三十三条　银行业金融机构应当按照要求向银行业监督管理机构报送反洗钱和反恐怖融资制度、年度报告、重大风险事项等材料，并对报送材料的及时性以及内容的真实性负责。

报送材料的内容和格式由国务院银行业监督管理机构统一规定。

第三十四条　银行业监督管理机构应当在职责范围内对银行业金融机构反洗钱和反恐怖融资义务履行情况依法开展现场检查。现场检查可以开展专项检查，或者与其他检查项目结合进行。

银行业监督管理机构可以与反洗钱行政主管部门开展联合检查。

第三十五条　银行业监督管理机构应当在职责范围内对银行业金融机构反洗钱和反恐怖融资义务履行情况进行评价，并将评价结果作为对银行业金融机构进行监管评级的重要因素。

第三十六条　银行业监督管理机构在市场准入工作中应当依法对银行业金融机构法人机构设立、分支机构设立、股权变更、变更注册资本、调整业务范围和增加业务品种、董事及高级管理人员任职资格许可进行反洗钱和反恐怖融资审查，对不符合条件的，不予批准。

第三十七条　银行业监督管理机构在市场准入工作中应当严格审核发起人、股东、实际控制人、最终受益人和董事、高级管理人员背景，审查资金来源和渠道，从源头上防止不法分子通过创设机构进行洗钱、恐怖融资活动。

第三十八条　设立银行业金融机构应当符合以下反洗钱和反恐怖融资审查条件：

（一）投资资金来源合法；

（二）股东及其控股股东、实际控制人、关联方、一致行动人、最终受益人等各方关系清晰透明，不得有故意或重大过失犯罪记录；

（三）建立反洗钱和反恐怖融资内部控制制度；

（四）设置反洗钱和反恐怖融资专门工作机构或指定内设机构负责该项工作；

（五）配备反洗钱和反恐怖融资专业人员，专业人员接受了必要的反洗钱和反恐怖融资培训；

（六）信息系统建设满足反洗钱和反恐怖融资要求；

（七）国务院银行业监督管理机构规定的其他条件。

第三十九条　设立银行业金融机构境内分支机构应当符合下列反洗钱和反恐怖融资审

查条件：

（一）总行具备健全的反洗钱和反恐怖融资内部控制制度并对分支机构具有良好的管控能力；

（二）总行的信息系统建设能够支持分支机构的反洗钱和反恐怖融资工作；

（三）拟设分支机构设置了反洗钱和反恐怖融资专门机构或指定内设机构负责反洗钱和反恐怖融资工作；

（四）拟设分支机构配备反洗钱和反恐怖融资专业人员，专业人员接受了必要的反洗钱和反恐怖融资培训；

（五）国务院银行业监督管理机构规定的其他条件。

第四十条　银行业金融机构申请投资设立、参股、收购境内法人金融机构的，申请人应当具备健全的反洗钱和反恐怖融资内部控制制度。

第四十一条　银行业金融机构申请投资设立、参股、收购境外金融机构的，应当具备健全的反洗钱和反恐怖融资内部控制制度，具有符合境外反洗钱和反恐怖融资监管要求的专业人才队伍。

第四十二条　银行业金融机构股东应当确保资金来源合法，不得以犯罪所得资金等不符合法律、行政法规及监管规定的资金入股。银行业金融机构应当知悉股东入股资金来源，在发生股权变更或者变更注册资本时应当按照要求向银行业监督管理机构报批或者报告。

第四十三条　银行业金融机构开展新业务需要经银行业监督管理机构批准的，应当提交新业务的洗钱和恐怖融资风险评估报告。银行业监督管理机构在进行业务准入时，应当对新业务的洗钱和恐怖融资风险评估情况进行审核。

第四十四条　申请银行业金融机构董事、高级管理人员任职资格，拟任人应当具备以下条件：

（一）不得有故意或重大过失犯罪记录；

（二）熟悉反洗钱和反恐怖融资法律法规，接受了必要的反洗钱和反恐怖融资培训，通过银行业监督管理机构组织的包含反洗钱和反恐怖融资内容的任职资格测试。

须经任职资格审核的银行业金融机构境外机构董事、高级管理人员应当熟悉境外反洗钱和反恐怖融资法律法规，具备相应反洗钱和反恐怖融资履职能力。

银行业金融机构董事、高级管理人员任职资格申请材料中应当包括接受反洗钱和反恐怖融资培训情况报告及本人签字的履行反洗钱和反恐怖融资义务的承诺书。

第四十五条　国务院银行业监督管理机构的各省级派出机构应当于每年第一季度末按

照要求向国务院银行业监督管理机构报送上年度反洗钱和反恐怖融资工作报告，包括反洗钱和反恐怖融资市场准入工作审核情况、现场检查及非现场监管情况、辖内银行业金融机构反洗钱和反恐怖融资工作情况等。

第四十六条　国务院银行业监督管理机构应当加强与境外监管当局的沟通与交流，通过签订监管合作协议、举行双边监管磋商和召开监管联席会议等形式加强跨境反洗钱和反恐怖融资监管合作。

第四十七条　银行业监督管理机构应当在职责范围内定期开展对银行业金融机构境外机构洗钱和恐怖融资风险管理情况的监测分析。监管机构应当将境外机构洗钱和恐怖融资风险管理情况作为与银行业金融机构监管会谈及外部审计会谈的重要内容。

第四十八条　银行业监督管理机构应当在职责范围内对银行业金融机构境外机构洗钱和恐怖融资风险管理情况依法开展现场检查，对存在问题的境外机构及时采取监管措施，并对违规机构依法依规进行处罚。

第四章　法律责任

第四十九条　银行业金融机构违反本办法规定，有下列情形之一的，银行业监督管理机构可以根据《中华人民共和国银行业监督管理法》规定采取监管措施或者对其进行处罚：

（一）未按规定建立反洗钱和反恐怖融资内部控制制度的；

（二）未有效执行反洗钱和反恐怖融资内部控制制度的；

（三）未按照规定设立反洗钱和反恐怖融资专门机构或者指定内设机构负责反洗钱和反恐怖融资工作的；

（四）未按照规定履行其他反洗钱和反恐怖融资义务的。

第五十条　银行业金融机构未按本办法第三十三条规定报送相关材料的，银行业监督管理机构可以根据《中华人民共和国银行业监督管理法》第四十六条、四十七条规定对其进行处罚。

第五十一条　对于反洗钱行政主管部门提出的处罚或者其他建议，银行业监督管理机构应当依法予以处理。

第五十二条　银行业金融机构或者其工作人员参与洗钱、恐怖融资等违法犯罪活动构成犯罪的，依法追究其刑事责任。

第五章　附　则

第五十三条　本办法由国务院银行业监督管理机构负责解释。

第五十四条　行业自律组织制定的反洗钱和反恐怖融资行业规则等应当向银行业监督

管理机构报告。

第五十五条　本办法自公布之日起施行。

中国人民银行金融消费者权益保护实施办法

基本信息：

【发布机关】中国人民银行

【发文字号】中国人民银行令〔2020〕第5号

【发布日期】2020.09.15

【时效性】现行有效

【效力级别】部门规章

【实施日期】2020.11.01

中国人民银行金融消费者权益保护实施办法

第一章　总　则

第一条　为了保护金融消费者合法权益，规范金融机构提供金融产品和服务的行为，维护公平、公正的市场环境，促进金融市场健康稳定运行，根据《中华人民共和国中国人民银行法》《中华人民共和国商业银行法》《中华人民共和国消费者权益保护法》和《国务院办公厅关于加强金融消费者权益保护工作的指导意见》（国办发〔2015〕81号）等，制定本办法。

第二条　在中华人民共和国境内依法设立的为金融消费者提供金融产品或者服务的银行业金融机构（以下简称银行），开展与下列业务相关的金融消费者权益保护工作，适用本办法：

（一）与利率管理相关的。

（二）与人民币管理相关的。

（三）与外汇管理相关的。

（四）与黄金市场管理相关的。

（五）与国库管理相关的。

（六）与支付、清算管理相关的。

（七）与反洗钱管理相关的。

（八）与征信管理相关的。

（九）与上述第一项至第八项业务相关的金融营销宣传和消费者金融信息保护。

（十）其他法律、行政法规规定的中国人民银行职责范围内的金融消费者权益保护工作。

在中华人民共和国境内依法设立的非银行支付机构（以下简称支付机构）提供支付服务的，适用本办法。

本办法所称金融消费者是指购买、使用银行、支付机构提供的金融产品或者服务的自然人。

第三条　银行、支付机构向金融消费者提供金融产品或者服务，应当遵循自愿、平等、公平、诚实信用的原则，切实承担金融消费者合法权益保护的主体责任，履行金融消费者权益保护的法定义务。

第四条　金融消费者应当文明、理性进行金融消费，提高自我保护意识，诚实守信，依法维护自身的合法权益。

第五条　中国人民银行及其分支机构坚持公平、公正原则，依法开展职责范围内的金融消费者权益保护工作，依法保护金融消费者合法权益。

中国人民银行及其分支机构会同有关部门推动建立和完善金融机构自治、行业自律、金融监管和社会监督相结合的金融消费者权益保护共同治理体系。

第六条　鼓励金融消费者和银行、支付机构充分运用调解、仲裁等方式解决金融消费纠纷。

第二章　金融机构行为规范

第七条　银行、支付机构应当将金融消费者权益保护纳入公司治理、企业文化建设和经营发展战略，制定本机构金融消费者权益保护工作的总体规划和具体工作措施。建立金融消费者权益保护专职部门或者指定牵头部门，明确部门及人员职责，确保部门有足够的人力、物力能够独立开展工作，并定期向高级管理层、董（理）事会汇报工作开展情况。

第八条　银行、支付机构应当落实法律法规和相关监管规定关于金融消费者权益保护的相关要求，建立健全金融消费者权益保护的各项内控制度：

（一）金融消费者权益保护工作考核评价制度。

（二）金融消费者风险等级评估制度。

（三）消费者金融信息保护制度。

（四）金融产品和服务信息披露、查询制度。

（五）金融营销宣传管理制度。

（六）金融知识普及和金融消费者教育制度。

（七）金融消费者投诉处理制度。

（八）金融消费者权益保护工作内部监督和责任追究制度。

（九）金融消费者权益保护重大事件应急制度。

（十）中国人民银行明确规定应当建立的其他金融消费者权益保护工作制度。

第九条　银行、支付机构应当建立健全涉及金融消费者权益保护工作的全流程管控机制，确保在金融产品或者服务的设计开发、营销推介及售后管理等各个业务环节有效落实金融消费者权益保护工作的相关规定和要求。全流程管控机制包括但不限于下列内容:

（一）事前审查机制。银行、支付机构应当实行金融消费者权益保护事前审查，及时发现并更正金融产品或者服务中可能损害金融消费者合法权益的问题，有效督办落实金融消费者权益保护审查意见。

（二）事中管控机制。银行、支付机构应当履行金融产品或者服务营销宣传中须遵循的基本程序和标准，加强对营销宣传行为的监测与管控。

（三）事后监督机制。银行、支付机构应当做好金融产品和服务的售后管理，及时调整存在问题或者隐患的金融产品和服务规则。

第十条　银行、支付机构应当开展金融消费者权益保护工作人员培训，增强工作人员的金融消费者权益保护意识和能力。

银行、支付机构应当每年至少开展一次金融消费者权益保护专题培训，培训对象应当全面覆盖中高级管理人员、基层业务人员及新入职人员。对金融消费者投诉多发、风险较高的业务岗位，应当适当提高培训的频次。

第十一条　银行、支付机构开展考核评价时，应当将金融消费者权益保护工作作为重要内容，并合理分配相关指标的占比和权重，综合考虑业务合规性、客户满意度、投诉处理及时率与合格率等，不得简单以投诉数量作为考核指标。

第十二条　银行、支付机构应当根据金融产品或者服务的特性评估其对金融消费者的适合度，合理划分金融产品和服务风险等级以及金融消费者风险承受等级，将合适的金融产品或者服务提供给适当的金融消费者。

第十三条　银行、支付机构应当依法保障金融消费者在购买、使用金融产品和服务时的财产安全，不得挪用、非法占用金融消费者资金及其他金融资产。

第十四条　银行、支付机构应当尊重社会公德，尊重金融消费者的人格尊严和民族风俗习惯，不得因金融消费者性别、年龄、种族、民族或者国籍等不同实行歧视性差别对待，不得使用歧视性或者违背公序良俗的表述。

第十五条　银行、支付机构应当尊重金融消费者购买金融产品或者服务的真实意愿，不得擅自代理金融消费者办理业务，不得擅自修改金融消费者的业务指令，不得强制搭售其他产品或者服务。

第十六条　银行、支付机构应当依据金融产品或者服务的特性，及时、真实、准确、全面地向金融消费者披露下列重要内容：

（一）金融消费者对该金融产品或者服务的权利和义务，订立、变更、中止和解除合同的方式及限制。

（二）银行、支付机构对该金融产品或者服务的权利、义务及法律责任。

（三）贷款产品的年化利率。

（四）金融消费者应当负担的费用及违约金，包括金额的确定方式，交易时间和交易方式。

（五）因金融产品或者服务产生纠纷的处理及投诉途径。

（六）银行、支付机构对该金融产品或者服务所执行的强制性标准、推荐性标准、团体标准或者企业标准的编号和名称。

（七）在金融产品说明书或者服务协议中，实际承担合同义务的经营主体完整的中文名称。

（八）其他可能影响金融消费者决策的信息。

第十七条　银行、支付机构对金融产品和服务进行信息披露时，应当使用有利于金融消费者接收、理解的方式。对利率、费用、收益及风险等与金融消费者切身利益相关的重要信息，应当根据金融产品或者服务的复杂程度及风险等级，对其中关键的专业术语进行解释说明，并以适当方式供金融消费者确认其已接收完整信息。

第十八条　银行、支付机构向金融消费者说明重要内容和披露风险时，应当依照法律法规和监管规定留存相关资料，自业务关系终止之日起留存时间不得少于 3 年。法律、行政法规另有规定的，从其规定。

留存的资料包括但不限于：

（一）金融消费者确认的金融产品说明书或者服务协议。

（二）金融消费者确认的风险提示书。

（三）记录向金融消费者说明重要内容的录音、录像资料或者系统日志等相关数据电文资料。

第十九条　银行、支付机构不得利用技术手段、优势地位，强制或者变相强制金融消

费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务。

第二十条　银行、支付机构在提供金融产品或者服务的过程中，不得通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务。

第二十一条　银行、支付机构向金融消费者提供金融产品或者服务时使用格式条款的，应当以足以引起金融消费者注意的字体、字号、颜色、符号、标识等显著方式，提请金融消费者注意金融产品或者服务的数量、利率、费用、履行期限和方式、注意事项、风险提示、纠纷解决等与金融消费者有重大利害关系的内容，并按照金融消费者的要求予以说明。格式条款采用电子形式的，应当可被识别且易于获取。

银行、支付机构不得以通知、声明、告示等格式条款的方式作出含有下列内容的规定：

（一）减轻或者免除银行、支付机构造成金融消费者财产损失的赔偿责任。

（二）规定金融消费者承担超过法定限额的违约金或者损害赔偿金。

（三）排除或者限制金融消费者依法对其金融信息进行查询、删除、修改的权利；

（四）排除或者限制金融消费者选择同业机构提供的金融产品或者服务的权利。

（五）其他对金融消费者不公平、不合理的规定。

银行、支付机构应当对存在侵害金融消费者合法权益问题或者隐患的格式条款和服务协议文本及时进行修订或者清理。

第二十二条　银行、支付机构应当对营销宣传内容的真实性负责。银行、支付机构实际承担的义务不得低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准。

前款“广告、资料或者说明”是指以营销为目的，利用各种传播媒体、宣传工具或者方式，就银行、支付机构的金融产品或者服务进行直接或者间接的宣传、推广等。

第二十三条　银行、支付机构在进行营销宣传活动时，不得有下列行为：

（一）虚假、欺诈、隐瞒或者引人误解的宣传。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺。

（五）其他违反金融消费者权益保护相关法律法规和监管规定的行为。

第二十四条　银行、支付机构应当切实承担金融知识普及和金融消费者教育的主体责任，提高金融消费者对金融产品和服务的认知能力，提升金融消费者金融素养和诚实守信意识。

银行、支付机构应当制定年度金融知识普及与金融消费者教育工作计划，结合自身特点开展日常性金融知识普及与金融消费者教育活动，积极参与中国人民银行及其分支机构组织的金融知识普及活动。银行、支付机构不得以营销金融产品或者服务替代金融知识普及与金融消费者教育。

第二十五条　银行、支付机构应当重视金融消费者需求的多元性与差异性，积极支持普惠金融重点目标群体获得必要、及时的基本金融产品和服务。

第二十六条　出现侵害金融消费者合法权益重大事件的，银行、支付机构应当根据重大事项报告的相关规定及时向中国人民银行或其分支机构报告。

第二十七条　银行、支付机构应当配合中国人民银行及其分支机构开展金融消费者权益保护领域的相关工作，按照规定报送相关资料。

第三章　消费者金融信息保护

第二十八条　本办法所称消费者金融信息，是指银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。

消费者金融信息的处理包括消费者金融信息的收集、存储、使用、加工、传输、提供、公开等。

第二十九条　银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者或者其监护人明示同意，但是法律、行政法规另有规定的除外。银行、支付机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集消费者金融信息，不得变相强制收集消费者金融信息。银行、支付机构不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外。

金融消费者不能或者拒绝提供必要信息，致使银行、支付机构无法履行反洗钱义务的，银行、支付机构可以根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，银行、支付机构可以依法拒绝提供金融产品或者服务。

第三十条　银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于

上述目的；金融消费者不同意的，银行、支付机构不得因此拒绝提供金融产品或者服务。银行、支付机构向金融消费者发送金融营销信息的，应当向其提供拒绝继续接收金融营销信息的方式。

第三十一条　银行、支付机构应当履行《中华人民共和国消费者权益保护法》第二十九条规定的明示义务，公开收集、使用消费者金融信息的规则，明示收集、使用消费者金融信息的目的、方式和范围，并留存有关证明资料。

银行、支付机构通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费者提示该同意的可能后果。

第三十二条　银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。

第三十三条　银行、支付机构应当建立以分级授权为核心的消费者金融信息使用管理制度，根据消费者金融信息的重要性、敏感度及业务开展需要，在不影响本机构履行反洗钱等法定义务的前提下，合理确定本机构工作人员调取信息的范围、权限，严格落实信息使用授权审批程序。

第三十四条　银行、支付机构应当按照国家档案管理和电子数据管理等规定，采取技术措施和其他必要措施，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。

银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄露、毁损、丢失时，银行、支付机构应当立即采取补救措施；信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在 72 小时以内报告银行、支付机构住所地的中国人民银行分支机构。中国人民银行分支机构接到报告后，视情况按照本办法第五十五条规定处理。

第四章　金融消费争议解决

第三十五条　金融消费者与银行、支付机构发生金融消费争议的，鼓励金融消费者先向银行、支付机构投诉，鼓励当事人平等协商，自行和解。

金融消费者应当依法通过正当途径客观、理性反映诉求，不扰乱正常的金融秩序和社会公共秩序。

本办法所称金融消费争议，是指金融消费者与银行、支付机构因购买、使用金融产品

或者服务所产生的民事争议。

第三十六条　银行、支付机构应当切实履行金融消费投诉处理的主体责任，银行、支付机构的法人机构应当按年度向社会发布金融消费者投诉数据和相关分析报告。

第三十七条　银行、支付机构应当通过金融消费者方便获取的渠道公示本机构的投诉受理方式，包括但不限于营业场所、官方网站首页、移动应用程序的醒目位置及客服电话主要菜单语音提示等。

第三十八条　银行、支付机构应当按照中国人民银行要求，加强对金融消费者投诉处理信息系统的建设与管理，对投诉进行正确分类并按时报送相关信息，不得迟报、漏报、谎报、错报或者瞒报投诉数据。

第三十九条　银行、支付机构收到金融消费者投诉后，依照相关法律法规和合同约定进行处理，并告知投诉人处理情况，但因投诉人原因导致无法告知的除外。

第四十条　中国人民银行分支机构设立投诉转办服务渠道。金融消费者对银行、支付机构作出的投诉处理不接受的，可以通过银行、支付机构住所地、合同签订地或者经营行为发生地中国人民银行分支机构进行投诉。

通过电子商务、网络交易购买、使用金融产品或者服务的，金融消费者通过银行、支付机构住所地的中国人民银行分支机构进行投诉。

第四十一条　金融消费者通过中国人民银行分支机构进行投诉，应当提供以下信息：姓名，有效身份证件信息，联系方式，明确的投诉对象及其住所地，具体的投诉请求、事实和理由。

金融消费者可以本人提出投诉，也可以委托他人代为提出投诉。以来信来访方式进行委托投诉的，应当向中国人民银行分支机构提交前款规定的投诉材料、授权委托书原件、委托人和受托人的身份证明。授权委托书应当载明受托人、委托事项、权限和期限，并由委托人本人签名。

第四十二条　中国人民银行分支机构对下列投诉不予接收：

（一）投诉人投诉的机构、产品或者服务不属于中国人民银行监管范围的。

（二）投诉人未提供真实身份，或者没有明确的被投诉人、没有具体的投诉请求和事实依据的。

（三）投诉人并非金融消费者本人，也未经金融消费者本人委托的。

（四）人民法院、仲裁机构、其他金融管理部门、行政部门或者依法设立的调解组织已经受理、接收或者处理的。

（五）双方达成和解协议并已经执行，没有新情况、新理由的。

（六）被投诉机构已提供公平合理的解决方案，投诉人就同一事项再次向中国人民银行分支机构投诉的。

（七）其他不符合法律、行政法规、规章有关规定的。

第四十三条　中国人民银行分支机构收到金融消费者投诉的，应当自收到投诉之日起7个工作日内作出下列处理:

（一）对投诉人和被投诉机构信息、投诉请求、事实和理由等进行登记。

（二）作出是否接收投诉的决定。决定不予接收的，应当告知投诉人。

（三）决定接收投诉的，应当将投诉转交被投诉机构处理或者转交金融消费纠纷调解组织提供调解服务。

需要投诉人对投诉内容进行补正的，处理时限于补正完成之日起计算。

银行、支付机构应当自收到中国人民银行分支机构转交的投诉之日起 15 日内答复投诉人。情况复杂的，经本机构投诉处理工作负责人批准，可以延长处理期限，并告知投诉人延长处理期限的理由，但最长处理期限不得超过 60 日。

第四十四条　银行、支付机构收到中国人民银行分支机构转交的投诉，应当按要求向中国人民银行分支机构反馈投诉处理情况。

反馈的内容包括投诉基本情况、争议焦点、调查结果及证据、处理依据、与金融消费者的沟通情况、延期处理情况及投诉人满意度等。

银行、支付机构应当妥善保存投诉资料，投诉资料留存时间自投诉办结之日起不得少于 3 年。法律、行政法规另有规定的，从其规定。

第四十五条　银行、支付机构、金融消费者可以向调解组织申请调解、中立评估。调解组织受理调解、中立评估申请后，可在合理、必要范围内请求当事人协助或者提供相关文件、资料。

本办法所称中立评估，是指调解组织聘请独立专家就争议解决提出参考性建议的行为。

第四十六条　金融消费纠纷调解组织应当依照法律、行政法规、规章及其章程的规定，组织开展金融消费纠纷调解、中立评估等工作，对银行、支付机构和金融消费者进行金融知识普及和教育宣传引导。

第五章　监督与管理机制

第四十七条　中国人民银行综合研究金融消费者保护重大问题，负责拟定发展规划和业务标准，建立健全金融消费者保护基本制度。

第四十八条　中国人民银行及其分支机构与其他金融管理部门、地方政府有关部门建立健全金融消费者权益保护工作协调机制，加强跨市场跨业态跨区域金融消费者权益保护的监管，强化信息共享和部门间沟通协作。

第四十九条　中国人民银行及其分支机构统筹开展金融消费者教育，引导、督促银行、支付机构开展金融知识普及宣传活动，协调推进金融知识纳入国民教育体系，组织开展消费者金融素养调查。

第五十条　中国人民银行及其分支机构会同有关部门构建监管执法合作机制，探索合作开展金融消费者权益保护监督检查、评估等具体工作。

第五十一条　中国人民银行及其分支机构牵头构建非诉第三方解决机制，鼓励、支持金融消费者权益保护社会组织依法履行职责，推动构建公正、高效、便捷的多元化金融消费纠纷解决体系。

第五十二条　中国人民银行及其分支机构协调推进相关普惠金融工作，建立健全普惠金融工作机制，指导、督促银行、支付机构落实普惠金融发展战略，组织开展职责范围内的普惠金融具体工作。

第五十三条　中国人民银行及其分支机构对金融消费者投诉信息进行汇总和分析，根据汇总和分析结果适时优化金融消费者权益保护监督管理方式、金融机构行为规范等。

第五十四条　中国人民银行及其分支机构可以采取下列措施，依法在职责范围内开展对银行、支付机构金融消费者权益保护工作的监督检查：

（一）进入被监管机构进行检查。

（二）询问被监管机构的工作人员，要求其对有关检查事项作出说明。

（三）查阅、复制被监管机构与检查事项有关的文件、资料，对可能被转移、隐匿或者毁损的文件、资料予以登记保存。

（四）检查被监管机构的计算机网络与信息系统。

进行现场检查时，检查人员不得少于二人，并应当出示合法证件和检查通知书。

银行、支付机构应当积极配合中国人民银行及其分支机构的现场检查和非现场检查，如实提供有关资料，不得拒绝、阻挠、逃避检查，不得谎报、隐匿、销毁相关证据材料。

第五十五条　银行、支付机构有侵害金融消费者合法权益行为的，中国人民银行及其分支机构可以对其采取下列措施：

（一）要求提交书面说明或者承诺。

（二）约见谈话。

（三）责令限期整改。

（四）视情将相关信息向其上级机构、行业监管部门反馈，在行业范围内发布，或者向社会公布。

（五）建议银行、支付机构对直接负责的董事、高级管理人员和其他直接责任人员给予处分。

（六）依法查处或者建议其他行政管理部门依法查处。

（七）中国人民银行职责范围内依法可以采取的其他措施。

第五十六条　中国人民银行及其分支机构组织开展银行、支付机构履行金融消费者权益保护义务情况的评估工作。

评估工作以银行、支付机构自评估为基础。银行、支付机构应当按年度进行自评估，并于次年 1 月 31 日前向中国人民银行或其分支机构报送自评估报告。

中国人民银行及其分支机构根据日常监督管理、投诉管理以及银行、支付机构自评估等情况进行非现场评估，必要时可以进行现场评估。

第五十七条　中国人民银行及其分支机构可以根据具体情况开展金融消费者权益保护环境评估工作。

第五十八条　中国人民银行及其分支机构建立金融消费者权益保护案例库制度，按照预防为先、教育为主的原则向银行、支付机构和金融消费者进行风险提示。

第五十九条　中国人民银行及其分支机构对于涉及金融消费者权益保护的重大突发事件，应当按照有关规定做好相关应急处置工作。

第六章　法律责任

第六十条　银行、支付机构有下列情形之一，侵害消费者金融信息依法得到保护的权利的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

（一）未经金融消费者明示同意，收集、使用其金融信息的。

（二）收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。

（三）未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。

（四）超出法律法规规定和双方约定的用途使用消费者金融信息的。

（五）未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信

息使用授权审批程序的。

（六）未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。

第六十一条　银行、支付机构有下列情形之一，对金融产品或者服务作出虚假或者引人误解的宣传的，中国人民银行或其分支机构应当在职责范围内依照《中华人民共和国消费者权益保护法》第五十六条的规定予以处罚：

（一）实际承担的义务低于在营销宣传活动中通过广告、资料或者说明等形式对金融消费者所承诺的标准的。

（二）引用不真实、不准确的数据和资料或者隐瞒限制条件等，对过往业绩或者产品收益进行夸大表述的。

（三）利用金融管理部门对金融产品或者服务的审核或者备案程序，误导金融消费者认为金融管理部门已对该金融产品或者服务提供保证的。

（四）明示或者暗示保本、无风险或者保收益等，对非保本投资型金融产品的未来效果、收益或者相关情况作出保证性承诺的。

第六十二条　银行、支付机构违反本办法规定，有下列情形之一，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款：

（一）未建立金融消费者权益保护专职部门或者指定牵头部门，或者金融消费者权益保护部门没有足够的人力、物力独立开展工作的。

（二）擅自代理金融消费者办理业务，擅自修改金融消费者的业务指令，或者强制搭售其他产品或者服务的。

（三）未按要求向金融消费者披露与金融产品和服务有关的重要内容的。

（四）利用技术手段、优势地位，强制或者变相强制金融消费者接受金融产品或者服务，或者排除、限制金融消费者接受同业机构提供的金融产品或者服务的。

（五）通过附加限制性条件的方式要求金融消费者购买、使用协议中未作明确要求的产品或者服务的。

（六）未按要求使用格式条款的。

（七）出现侵害金融消费者合法权益重大事件未及时向中国人民银行或其分支机构报告的。

（八）不配合中国人民银行及其分支机构开展金融消费者权益保护领域相关工作，或

者未按照规定报送相关资料的。

（九）未按要求对金融消费者投诉进行正确分类，或者迟报、漏报、谎报、错报、瞒报投诉数据的。

（十）收到中国人民银行分支机构转交的投诉后，未在规定期限内答复投诉人，或者未按要求向中国人民银行分支机构反馈投诉处理情况的。

（十一）拒绝、阻挠、逃避检查，或者谎报、隐匿、销毁相关证据材料的。

第六十三条　对银行、支付机构侵害金融消费者权益重大案件负有直接责任的董事、高级管理人员和其他直接责任人员，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款。

第六十四条　中国人民银行及其分支机构的工作人员在开展金融消费者权益保护工作过程中有下列情形之一的，依法给予处分；涉嫌构成犯罪的，移送司法机关依法追究刑事责任：

（一）违反规定对银行、支付机构进行检查的。

（二）泄露知悉的国家秘密或者商业秘密的。

（三）滥用职权、玩忽职守的其他行为。

第七章　附　则

第六十五条　商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构、个人本外币兑换特许业务经营机构参照适用本办法。法律、行政法规另有规定的，从其规定。

第六十六条　本办法中除“工作日”以外的“日”为自然日。

第六十七条　本办法由中国人民银行负责解释。

第六十八条　本办法自 2020 年 11 月 1 日起施行。《中国人民银行金融消费权益保护工作管理办法（试行）》（银办发〔2013〕107 号文印发）与《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314 号文印发）同时废止。

侵害消费者权益行为处罚办法

基本信息： 【发布机关】国家市场监督管理总局　　【时效性】 现行有效

【发文字号】国家市场监督管理总局令第 31 号
【效力级别】部门规章
【实施日期】2020.10.23
【发布日期】2020.10.23

侵害消费者权益行为处罚办法

第一条 为依法制止侵害消费者权益行为，保护消费者的合法权益，维护社会经济秩序，根据《消费者权益保护法》等法律法规，制定本办法。

第二条 市场监督管理部门依照《消费者权益保护法》等法律法规和本办法的规定，保护消费者为生活消费需要购买、使用商品或者接受服务的权益，对经营者侵害消费者权益的行为实施行政处罚。

第三条 市场监督管理部门依法对侵害消费者权益行为实施行政处罚，应当依照公正、公开、及时的原则，坚持处罚与教育相结合，综合运用建议、约谈、示范等方式实施行政指导，督促和指导经营者履行法定义务。

第四条 经营者为消费者提供商品或者服务，应当遵循自愿、平等、公平、诚实信用的原则，依照《消费者权益保护法》等法律法规的规定和与消费者的约定履行义务，不得侵害消费者合法权益。

第五条 经营者提供商品或者服务不得有下列行为：

（一）销售的商品或者提供的服务不符合保障人身、财产安全要求；

（二）销售失效、变质的商品；

（三）销售伪造产地、伪造或者冒用他人的厂名、厂址、篡改生产日期的商品；

（四）销售伪造或者冒用认证标志等质量标志的商品；

（五）销售的商品或者提供的服务侵犯他人注册商标专用权；

（六）销售伪造或者冒用知名商品特有的名称、包装、装潢的商品；

（七）在销售的商品中掺杂、掺假，以假充真，以次充好，以不合格商品冒充合格商品；

（八）销售国家明令淘汰并停止销售的商品；

（九）提供商品或者服务中故意使用不合格的计量器具或者破坏计量器具准确度；

（十）骗取消费者价款或者费用而不提供或者不按照约定提供商品或者服务。

第六条 经营者向消费者提供有关商品或者服务的信息应当真实、全面、准确，不得有下列虚假或者引人误解的宣传行为：

（一）不以真实名称和标记提供商品或者服务；

（二）以虚假或者引人误解的商品说明、商品标准、实物样品等方式销售商品或者服务；

（三）作虚假或者引人误解的现场说明和演示；

（四）采用虚构交易、虚标成交量、虚假评论或者雇佣他人等方式进行欺骗性销售诱导；

（五）以虚假的“清仓价”、“甩卖价”、“最低价”、“优惠价”或者其他欺骗性价格表示销售商品或者服务；

（六）以虚假的“有奖销售”、“还本销售”、“体验销售”等方式销售商品或者服务；

（七）谎称正品销售“处理品”、“残次品”、“等外品”等商品；

（八）夸大或隐瞒所提供的商品或者服务的数量、质量、性能等与消费者有重大利害关系的信息误导消费者；

（九）以其他虚假或者引人误解的宣传方式误导消费者。

第七条 经营者对市场监督管理部门责令其对提供的缺陷商品或者服务采取停止销售或者服务等措施，不得拒绝或者拖延。经营者未按照责令停止销售或者服务通知、公告要求采取措施的，视为拒绝或者拖延。

第八条 经营者提供商品或者服务，应当依照法律规定或者当事人约定承担修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失等民事责任，不得故意拖延或者无理拒绝消费者的合法要求。经营者有下列情形之一并超过十五日的，视为故意拖延或者无理拒绝：

（一）经有关行政部门依法认定为不合格商品，自消费者提出退货要求之日起未退货的；

（二）自国家规定、当事人约定期满之日起或者不符合质量要求的自消费者提出要求之日起，无正当理由拒不履行修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失等义务的。

第九条 经营者采用网络、电视、电话、邮购等方式销售商品，应当依照法律规定承担无理由退货义务，不得故意拖延或者无理拒绝。经营者有下列情形之一的，视为故意拖延或者无理拒绝：

（一）对于适用无理由退货的商品，自收到消费者退货要求之日起超过十五日未办理

退货手续，或者未向消费者提供真实、准确的退货地址、退货联系人等有效联系信息，致使消费者无法办理退货手续；

（二）未经消费者确认，以自行规定该商品不适用无理由退货为由拒绝退货；

（三）以消费者已拆封、查验影响商品完好为由拒绝退货；

（四）自收到退回商品之日起无正当理由超过十五日未向消费者返还已支付的商品价款。

第十条 经营者以预收款方式提供商品或者服务，应当与消费者明确约定商品或者服务的数量和质量、价款或者费用、履行期限和方式、安全注意事项和风险警示、售后服务、民事责任等内容。未按约定提供商品或者服务的，应当按照消费者的要求履行约定或者退回预付款，并应当承担预付款的利息、消费者必须支付的合理费用。对退款无约定的，按照有利于消费者的计算方式折算退款金额。

经营者对消费者提出的合理退款要求，明确表示不予退款，或者自约定期满之日起、无约定期限的自消费者提出退款要求之日起超过十五日未退款的，视为故意拖延或者无理拒绝。

第十一条 经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者不得有下列行为：

（一）未经消费者同意，收集、使用消费者个人信息；

（二）泄露、出售或者非法向他人提供所收集的消费者个人信息；

（三）未经消费者同意或者请求，或者消费者明确表示拒绝，向其发送商业性信息。

前款中的消费者个人信息是指经营者在提供商品或者服务活动中收集的消费者姓名、性别、职业、出生日期、身份证件号码、住址、联系方式、收入和财产状况、健康状况、消费情况等能够单独或者与其他信息结合识别消费者的信息。

第十二条 经营者向消费者提供商品或者服务使用格式条款、通知、声明、店堂告示等的，应当以显著方式提请消费者注意与消费者有重大利害关系的内容，并按照消费者的要求予以说明，不得作出含有下列内容的规定：

（一）免除或者部分免除经营者对其所提供的商品或者服务应当承担的修理、重作、更换、退货、补足商品数量、退还货款和服务费用、赔偿损失等责任；

（二）排除或者限制消费者提出修理、更换、退货、赔偿损失以及获得违约金和其他合理赔偿的权利；

（三）排除或者限制消费者依法投诉、举报、提起诉讼的权利；

（四）强制或者变相强制消费者购买和使用其提供的或者其指定的经营者提供的商品或者服务，对不接受其不合理条件的消费者拒绝提供相应商品或者服务，或者提高收费标准；

（五）规定经营者有权任意变更或者解除合同，限制消费者依法变更或者解除合同权利；

（六）规定经营者单方享有解释权或者最终解释权；

（七）其他对消费者不公平、不合理的规定。

第十三条 从事服务业的经营者不得有下列行为：

（一）从事为消费者提供修理、加工、安装、装饰装修等服务的经营者谎报用工用料，故意损坏、偷换零部件或材料，使用不符合国家质量标准或者与约定不相符的零部件或材料，更换不需要更换的零部件，或者偷工减料、加收费用，损害消费者权益的；

（二）从事房屋租赁、家政服务等中介服务的经营者提供虚假信息或者采取欺骗、恶意串通等手段损害消费者权益的。

第十四条 经营者有本办法第五条至第十一条规定的情形之一，其他法律、法规有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由市场监督管理部门依照《消费者权益保护法》第五十六条予以处罚。

第十五条 经营者违反本办法第十二条、第十三条规定，其他法律、法规有规定的，依照法律、法规的规定执行；法律、法规未作规定的，由市场监督管理部门责令改正，可以单处或者并处警告，违法所得三倍以下、但最高不超过三万元的罚款，没有违法所得的，处以一万元以下的罚款。

第十六条 经营者有本办法第五条第（一）项至第（六）项规定行为之一且不能证明自己并非欺骗、误导消费者而实施此种行为的，属于欺诈行为。

经营者有本办法第五条第（七）项至第（十）项、第六条和第十三条规定行为之一的，属于欺诈行为。

第十七条 经营者对市场监督管理部门作出的行政处罚决定不服的，可以依法申请行政复议或者提起行政诉讼。

第十八条 侵害消费者权益违法行为涉嫌犯罪的，市场监督管理部门应当按照有关规定，移送司法机关追究其刑事责任。

第十九条 市场监督管理部门依照法律法规及本办法规定对经营者予以行政处罚的，应当记入经营者的信用档案，并通过企业信用信息公示系统等及时向社会公布。

企业应当依据《企业信息公示暂行条例》的规定，通过企业信用信息公示系统及时向社会公布相关行政处罚信息。

第二十条 市场监督管理执法人员玩忽职守或者包庇经营者侵害消费者合法权益的行为的，应当依法给予行政处分；涉嫌犯罪的，依法移送司法机关。

第二十一条 本办法由国家市场监督管理总局负责解释。

第二十二条 本办法自 2015 年 3 月 15 日起施行。1996 年 3 月 15 日国家工商行政管理局发布的《欺诈消费者行为处罚办法》（国家工商行政管理局令第 50 号）同时废止。

征信业务管理办法

基本信息：	
【发布机关】中国人民银行	【时效性】暂未生效
【发文字号】中国人民银行令〔2021〕第 4 号	【效力级别】部门规章
【发布日期】2021.09.27	【实施日期】2022.01.01

征信业务管理办法

第一章 总则

第一条 为了规范征信业务及其相关活动，保护信息主体合法权益，促进征信业健康发展，推进社会信用体系建设，根据《中华人民共和国中国人民银行法》《中华人民共和国个人信息保护法》《征信业管理条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内，对法人和非法人组织（以下统称企业）、个人开展征信业务及其相关活动的，适用本办法。

第三条 本办法所称征信业务，是指对企业和个人的信用信息进行采集、整理、保存、加工，并向信息使用者提供的活动。

本办法所称信用信息，是指依法采集，为金融等活动提供服务，用于识别判断企业和个人信用状况的基本信息、借贷信息、其他相关信息，以及基于前述信息形成的分析评价信息。

第四条 从事个人征信业务的，应当依法取得中国人民银行个人征信机构许可；从事企业征信业务的，应当依法办理企业征信机构备案；从事信用评级业务的，应当依法办理信用评级机构备案。

第五条 金融机构不得与未取得合法征信业务资质的市场机构开展商业合作获取征信服

务。

本办法所称金融机构，是指国务院金融管理部门监督管理的从事金融业务的机构。

地方金融监管部门负责监督管理的地方金融组织适用本办法关于金融机构的规定。

第六条 从事征信业务及其相关活动，应当保护信息主体合法权益，保障信息安全，防范信用信息泄露、丢失、毁损或者被滥用，不得危害国家秘密，不得侵犯个人隐私和商业秘密。

从事征信业务及其相关活动，应当遵循独立、客观、公正的原则，不得违反法律法规的规定，不得违反社会公序良俗。

第二章 信用信息采集

第七条 采集个人信用信息，应当采取合法、正当的方式，遵循最小、必要的原则，不得过度采集。

第八条 征信机构不得以下列方式采集信用信息：

（一）欺骗、胁迫、诱导；

（二）向信息主体收费；

（三）从非法渠道采集；

（四）以其他侵害信息主体合法权益的方式。

第九条 信息提供者向征信机构提供信用信息的，征信机构应当制定相关制度，对信息提供者的信息来源、信息质量、信息安全、信息主体授权等进行必要的审查。

第十条 征信机构与信息提供者在开办业务及合作中应当遵守《中华人民共和国个人信息保护法》等法律法规，通过协议等形式明确信息采集的原则以及各自在获得客户同意、信息采集、加工处理、信息更正、异议处理、信息安全等方面的权利义务和责任。

第十一条 征信机构经营个人征信业务，应当制定采集个人信用信息的方案，并就采集的数据项、信息来源、采集方式、信息主体合法权益保护制度等事项及其变化向中国人民银行报告。

第十二条 征信机构采集个人信用信息应当经信息主体本人同意，并且明确告知信息主体采集信用信息的目的。依照法律法规公开的信息除外。

第十三条 征信机构通过信息提供者取得个人同意的，信息提供者应当向信息主体履行告知义务。

第十四条 个人征信机构应当将与其合作，进行个人信用信息采集、整理、加工和分析的信息提供者，向中国人民银行报告。

个人征信机构应当规范与信息提供者的合作协议内容。信息提供者应当就个人信用信息处理事项接受个人征信机构的风险评估和中国人民银行的情况核实。

第十五条 采集企业信用信息，应当基于合法的目的，不得侵犯商业秘密。

第三章 信用信息整理、保存、加工

第十六条 征信机构整理、保存、加工信用信息，应当遵循客观性原则，不得篡改原始信息。

第十七条 征信机构应当采取措施，提高征信系统信息的准确性，保障信息质量。

第十八条 征信机构在整理、保存、加工信用信息过程中发现信息错误的，如属于信息提供者报送错误的，应当及时通知信息提供者更正；如属于内部处理错误的，应当及时更正，并优化信用信息内部处理流程。

第十九条 征信机构应当对来自不同信息提供者的信息进行比对，发现信息不一致的，及时进行核查和处理。

第二十条 征信机构采集的个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年。

个人不良信息保存期限届满，征信机构应当将个人不良信息在对外服务和应用中删除；作为样本数据的，应当进行匿名化处理。

第四章 信用信息提供、使用

第二十一条 征信机构对外提供征信产品和服务，应当遵循公平性原则，不得设置不合理的商业条件限制不同的信息使用者使用，不得利用优势地位提供歧视性或者排他性的产品和服务。

第二十二条 征信机构应当采取适当的措施，对信息使用者的身份、业务资质、使用目的等进行必要的审查。

征信机构应当对信息使用者接入征信系统的网络和系统安全、合规性管理措施进行评估，对查询行为进行监测。发现安全隐患或者异常行为的，及时核查；发现违法违规行为的，停止提供服务。

第二十三条 信息使用者应当采取必要的措施，保障查询个人信用信息时取得信息主体的同意，并且按照约定用途使用个人信用信息。

第二十四条 信息使用者使用征信机构提供的信用信息，应当基于合法、正当的目的，不得滥用信用信息。

第二十五条 个人信息主体有权每年两次免费获取本人的信用报告，征信机构可以通过

互联网查询、营业场所查询等多种方式为个人信息主体提供信用报告查询服务。

第二十六条 信息主体认为信息存在错误、遗漏的，有权向征信机构或者信息提供者提出异议；认为侵害自身合法权益的，可以向所在地中国人民银行分支机构投诉。对异议和投诉按照《征信业管理条例》及相关规定办理。

第二十七条 征信机构不得以删除不良信息或者不采集不良信息为由，向信息主体收取费用。

第二十八条 征信机构提供信用报告等信用信息查询产品和服务的，应当客观展示查询的信用信息内容，并对查询的信用信息内容及专业名词进行解释说明。

信息主体有权要求征信机构在信用报告中添加异议标注和声明。

第二十九条 征信机构提供画像、评分、评级等信用评价类产品和服务的，应当建立评价标准，不得将与信息主体信用无关的要素作为评价标准。

征信机构正式对外提供信用评价类产品和服务前，应当履行必要的内部测试和评估验证程序，使评价规则可解释、信息来源可追溯。

征信机构提供经济主体或者债务融资工具信用评级产品和服务的，应当按照《信用评级业管理暂行办法》（中国人民银行 发展改革委 财政部 证监会令〔2019〕第 5 号发布）等相关规定开展业务。

第三十条 征信机构提供信用反欺诈产品和服务的，应当建立欺诈信用信息的认定标准。

第三十一条 征信机构提供信用信息查询、信用评价类、信用反欺诈产品和服务，应当向中国人民银行或其省会（首府）城市中心支行以上分支机构报告下列事项：

（一）信用报告的模板及内容；

（二）信用评价类产品和服务的评价方法、模型、主要维度要素；

（三）信用反欺诈产品和服务的数据来源、欺诈信用信息认定标准。

第三十二条 征信机构不得从事下列活动：

（一）对信用评价结果进行承诺；

（二）使用对信用评价结果有暗示性的内容宣传产品和服务；

（三）未经政府部门或者行业协会同意，假借其名义进行市场推广；

（四）以胁迫、欺骗、诱导的方式向信息主体或者信息使用者提供征信产品和服务；

（五）对征信产品和服务进行虚假宣传；

（六）提供其他影响征信业务客观公正性的征信产品和服务。

第五章 信用信息安全

第三十三条 征信机构应当落实网络安全等级保护制度，制定涉及业务活动和设备设施的安全管理制度，采取有效保护措施，保障征信系统的安全。

第三十四条 个人征信机构、保存或者处理 100 万户以上企业信用信息的企业征信机构，应当符合下列要求：

（一）核心业务信息系统网络安全保护等级具备三级或者三级以上安全保护能力；

（二）设立信息安全负责人和个人信息保护负责人，由公司章程规定的高级管理人员担任；

（三）设立专职部门，负责信息安全和个人信息保护工作，定期检查征信业务、系统安全、个人信息保护制度措施执行情况。

第三十五条 征信机构应当保障征信系统运行设施设备、安全控制设施设备以及互联网应用程序的安全，做好征信系统日常运维管理，保障系统物理安全、通信网络安全、区域边界安全、计算环境安全、管理中心安全等，防范征信系统受到非法入侵和破坏。

第三十六条 征信机构应当在人员录用、离岗、考核、安全教育、培训和外部人员访问管理等方面做好人员安全管理工作。

第三十七条 征信机构应当严格限定公司内部查询和获取信用信息的工作人员的权限和范围。

征信机构应当留存工作人员查询、获取信用信息的操作记录，明确记载工作人员查询和获取信用信息的时间、方式、内容及用途。

第三十八条 征信机构应当建立应急处置制度，在发生或者有可能发生信用信息泄露等事件时，立即采取必要措施降低危害，并及时向中国人民银行及其省会（首府）城市中心支行以上分支机构报告。

第三十九条 征信机构在中华人民共和国境内开展征信业务及其相关活动，采集的企业信用信息和个人信用信息应当存储在中华人民共和国境内。

第四十条 征信机构向境外提供个人信用信息，应当符合法律法规的规定。

征信机构向境外信息使用者提供企业信用信息查询产品和服务，应当对信息使用者的身份、信用信息用途进行必要的审查，确保信用信息用于跨境贸易、投融资等合理用途，不得危害国家安全。

第四十一条 征信机构与境外征信机构合作的，应当在合作协议签署后、业务开展前将合作协议报告中国人民银行。

第六章 监督管理

第四十二条 征信机构应当将下列事项向社会公开，接受社会监督：

（一）采集的信用信息类别；

（二）信用报告的基本格式内容；

（三）异议处理流程；

（四）中国人民银行认为需要公开的其他事项。

第四十三条 个人征信机构应当每年对自身个人征信业务遵守《中华人民共和国个人信息保护法》《征信业管理条例》的情况进行合规审计，并将合规审计报告及时报告中国人民银行。

第四十四条 中国人民银行及其省会（首府）城市中心支行以上分支机构对征信机构的下列事项进行监督检查：

（一）征信内控制度建设，包括各项制度和相关规程的齐备性、合规性和可操作性等；

（二）征信业务合规经营情况，包括采集信用信息、对外提供和使用信用信息、异议与投诉处理、用户管理、其他事项合规性等；

（三）征信系统安全情况，包括信息技术制度、安全管理、系统开发等；

（四）与征信业务活动相关的其他事项。

第四十五条 信息提供者和信息使用者违反《征信业管理条例》规定，侵犯信息主体合法权益的，由中国人民银行及其省会（首府）城市中心支行以上分支机构依法对其检查和处理。

第七章 法律责任

第四十六条 违反本办法第四条规定，擅自从事个人征信业务的，由中国人民银行按照《征信业管理条例》第三十六条进行处罚；擅自从事企业征信业务的，由中国人民银行省会（首府）城市中心支行以上分支机构按照《征信业管理条例》第三十七条进行处罚。

金融机构违反本办法第五条规定，与未取得合法征信业务资质的市场机构开展商业合作获取征信服务的，由中国人民银行及其分支机构责令改正，对单位处 3 万元以下罚款，对直接负责的主管人员处 1000 元以下罚款。

第四十七条 征信机构违反本办法第八条、第十六条、第二十条、第二十七条、第三十二条规定的，由中国人民银行及其省会（首府）城市中心支行以上分支机构按照《征信业管理条例》第三十八条进行处罚。

第四十八条 征信机构违反本办法第十四条、第二十一条、第三十一条、第三十四条、

第三十九条、第四十二条规定的，由中国人民银行及其省会（首府）城市中心支行以上分支机构责令改正，没收违法所得，对单位处 3 万元以下罚款，对直接负责的主管人员处 1000 元以下罚款。法律、行政法规另有规定的，依照其规定。

第八章 附则

第四十九条 金融信用信息基础数据库从事征信业务、从事信贷业务的机构向金融信用信息基础数据库报送或者查询信用信息参照本办法执行。

第五十条 以“信用信息服务”“信用服务”“信用评分”“信用评级”“信用修复”等名义对外实质提供征信服务的，适用本办法。

第五十一条 本办法施行前未取得个人征信业务经营许可或者未进行企业征信机构备案但实质从事征信业务的机构，应当自本办法施行之日起 18 个月内完成合规整改。

第五十二条 本办法由中国人民银行负责解释。

第五十三条 本办法自 2022 年 1 月 1 日起施行。

（四）规范性文件

电子银行安全评估指引

基本信息：	
【发布机关】中国银行业监督管理委员会	【时效性】现行有效
【发文字号】银监发〔2006〕第 9 号	【效力级别】部门规章
【发布日期】2006.01.26	【实施日期】2006.03.01

电子银行安全评估指引

第一章　总　则

第一条　为加强电子银行业务的安全与风险管理，保证电子银行安全评估的客观性、及时性、全面性和有效性，依据《电子银行业务管理办法》的有关规定，制定本指引。

第二条　电子银行的安全评估，是指金融机构在开展电子银行业务过程中，对电子银行的安全策略、内控制度、风险管理、系统安全、客户保护等方面进行的安全测试和管控能力的考察与评价。

第三条　开展电子银行业务的金融机构，应根据其电子银行发展和管理的需要，至少每 2 年对电子银行进行一次全面的安全评估。

第四条　金融机构可以利用外部专业化的评估机构对电子银行进行安全评估，也可以利用内部独立于电子银行业务运营和管理部门的评估部门对电子银行进行安全评估。

第五条　金融机构应建立电子银行安全评估的规章制度体系和工作规程，保证电子银行安全评估能够及时、客观地得以实施。

第六条　金融机构的电子银行安全评估，应接受中国银行业监督管理委员会（以下简称中国银监会）的监督指导。

第二章　安全评估机构

第七条　承担金融机构电子银行安全评估工作的机构，可以是金融机构外部的社会专业化机构，也可以是金融机构内部具备相应条件的相对独立部门。

第八条　外部机构从事电子银行安全评估，应具备以下条件：

（一）具有较为完善的开展电子银行安全评估业务的管理制度和操作规程；

（二）制定了系统、全面的评估手册或评估指导文件，评估手册或评估指导文件的内容应至少包括评估程序、评估方法和依据、评估标准等；

（三）拥有与电子银行安全评估相关的各类专业人才，了解国际和中国相关行业的行

业标准；

（四） 中国银监会规定的其他从事电子银行安全评估应当具备的条件。

第九条 金融机构内部部门从事电子银行安全评估，除应具备第八条 规定的有关条件外，还应具备以下条件：

（一） 必须独立于电子银行业务系统开发部门、运营部门和管理部门；

（二） 未直接参与过有关电子银行设备的选购工作。

第十条 中国银监会负责电子银行安全评估机构资质认定工作。

电子银行安全评估机构在开展金融机构电子银行安全评估业务前，可以向中国银监会申请对其资质进行认定。

第十一条 金融机构在进行电子银行安全评估时，可以选择经中国银监会资质认定的安全评估机构，也可以选择未经中国银监会资质认定的安全评估机构。

金融机构选择经中国银监会资质认定的安全评估机构时，有关安全评估机构的管理适用本指引有关规定。金融机构选择未经中国银监会资质认定的安全评估机构时，安全评估机构的选择标准应不低于第八条、第九条规定的条件要求，并应按照《电子银行业务管理办法》的有关规定，报送相关材料。

电子银行安全评估机构无论是否经过中国银监会资质认定，在开展电子银行安全评估活动时，都应遵守有关电子银行安全评估实施和管理的规定。

第十二条 中国银监会每年将组织一次电子银行安全评估机构资质认定工作，评定时间应提前 1 个月公告。

第十三条 申请资质认定的电子银行安全评估机构，应在中国银监会公告规定的时限内提交以下材料（一式七份）：

（一） 电子银行安全评估资质认定申请报告；

（二） 机构介绍；

（三） 安全评估业务管理框架、管理制度、操作规程等；

（四） 评估手册或评估指导文件；

（五） 主要评估人员简历；

（六） 中国银监会要求提供的其他文件、资料。

第十四条 中国银监会收到安全评估机构资质认定申请完整材料后，组织有关专家和监管人员对申请材料进行评议，采用投票的办法评定电子银行安全评估机构是否达到了有

关资质要求。

第十五条　中国银监会对评估机构资质评议后，出具《电子银行安全评估机构资质认定意见书》，载明评议意见，对评估机构的资质做出认定。

第十六条　中国银监会出具的《电子银行安全评估机构资质认定意见书》，仅供评估机构与金融机构商恰有关电子银行安全评估业务时使用，不影响评估机构开展其他经营活动。

评估机构不得将《电子银行安全评估机构资质认定意见书》用于宣传或其他活动。

第十七条　经中国银监会评议并被认为达到有关资质要求的评估机构，每次资质认定的有效期限为 2 年。

经评议不符合认定资质的，评估机构可在下一年度重新申请资质认定。

第十八条　在资质认定的有效期限内，电子银行安全评估机构如果出现下列情况，中国银监会将撤销已做出的评议和认定意见：

（一）评估机构管理不善，其工作人员泄露被评估机构秘密的；

（二）评估工作质量低下，评估活动出现重要遗漏的；

（三）未按要求提交评估报告，或评估报告中存在不实表述的；

（四）将《电子银行安全评估机构资质认定意见书》用于宣传和其他经营活动的；

（五）存在其他严重不尽职行为的。

第十九条　评估机构有下列行为之一的，中国银监会将在一定期限或无限期不再受理评估机构的资质认定申请，金融机构不应再委托该评估机构进行安全评估：

（一）与委托机构合谋，共同隐瞒在安全评估过程中发现的安全漏洞，未按要求写入评估报告的；

（二）在评估过程中弄虚作假，编造安全评估报告的；

（三）泄漏被评估机构机密信息，或不当使用被评估机构机密资料的。

金融机构内部评估机构出现以上情况之一的，中国银监会将依法对相关机构和责任人进行处罚。

第二十条　中国银监会认可的电子银行安全评估机构，以及有关资质认定、撤销等信息，仅向开展电子银行业务的各金融机构通报，不向社会发布。

金融机构不得向第三方泄露中国银监会的有关通报信息，影响有关机构的其他业务活动，也不得将有关信息用于与电子银行安全评估活动无关的其他业务活动。

第二十一条　金融机构可以在中国银监会认定的评估机构范围内，自主选择电子银行安全评估机构。

第二十二条　电子银行主要系统设置于境外并在境外实施电子银行安全评估的外资金融机构，以及需要按照所在地监管部门的要求在境外实施电子银行安全评估的中资金融机构境外分支机构，电子银行安全评估机构的选择应遵循所在国家或地区的法律要求。

所在国家或地区没有相关法律要求的，金融机构应参照本指引的有关规定开展安全评估活动。

第二十三条　金融机构应与聘用的电子银行安全评估机构签订书面服务协议，在服务协议中，必须含有明确的保密条款和保密责任。

金融机构选择内部部门作为评估机构时，应由电子银行管理部门与评估部门签订评估责任确定书。

第二十四条　安全评估机构应根据评估协议的规定，认真履行评估职责，真实评估被评估机构电子银行安全状况。

第三章　安全评估的实施

第二十五条　评估机构在开始电子银行安全评估之前，应就评估的范围、重点、时间与要求等问题，与被评估机构进行充分的沟通，制定评估计划，由双方签字认可。

第二十六条　依据评估计划，评估机构进场对委托机构的电子银行安全进行评估。

电子银行安全评估应真实、全面地评价电子银行系统的安全性。

第二十七条　电子银行安全评估至少应包括以下内容：

（一）安全策略；

（二）内控制度建设；

（三）风险管理状况；

（四）系统安全性；

（五）电子银行业务运行连续性计划；

（六）电子银行业务运行应急计划；

（七）电子银行风险预警体系；

（八）其他重要安全环节和机制的管理。

第二十八条　电子银行安全策略的评估，至少应包括以下内容：

（一）安全策略制定的流程与合理性；

（二） 系统设计与开发的安全策略；

（三） 系统测试与验收的安全策略；

（四） 系统运行与维护的安全策略；

（五） 系统备份与应急的安全策略；

（六） 客户信息安全策略。

评估机构对金融机构安全策略的评估，不仅要评估安全策略、规章制度和程序是否存在，还要评估这些制度是否得到贯彻执行，是否及时更新，是否全面覆盖电子银行业务系统。

第二十九条　电子银行内控制度的评估，应至少包括以下内容：

（一） 内部控制体系总体建设的科学性与适宜性；

（二） 董事会和高级管理层在电子银行安全和风险管理体系中的职责，以及相关部门职责和责任的合理性；

（三） 安全监控机制的建设与运行情况；

（四） 内部审计制度的建设与运行情况。

第三十条　电子银行风险管理状况的评估，应至少包括以下内容：

（一） 电子银行风险管理架构的适应性和合理性；

（二） 董事会和高级管理层对电子银行安全与风险管理的认知能力与相关政策、策略的制定执行情况；

（三） 电子银行管理机构职责设置的合理性及对相关风险的管控能力；

（四） 管理人员配备与培训情况；

（五） 电子银行风险管理的规章制度与操作规定、程序等的执行情况；

（六） 电子银行业务的主要风险及管理状况；

（七） 业务外包管理制度建设与管理状况。

第三十一条　电子银行系统安全性的评估，应至少包括以下内容：

（一） 物理安全；

（二） 数据通讯安全；

（三） 应用系统安全；

（四） 密钥管理；

（五） 客户信息认证与保密；

（六） 入侵监测机制和报告反应机制。

评估机构应突出对数据通讯安全和应用系统安全的评估，客观评价金融机构是否采用了合适的加密技术、合理设计和配置了服务器和防火墙，银行内部运作系统和数据库是否安全等，以及金融机构是否制定了控制和管理修改电子银行系统的制度和控制程序，并能保证各种修改得到及时测试和审核。

第三十二条 电子银行业务运行连续性计划的评估，应至少包括以下内容：

（一） 保障业务连续运营的设备和系统能力；

（二） 保证业务连续运营的制度安排和执行情况。

第三十三条 电子银行业务运行应急计划的评估，应至少包括以下内容：

（一） 电子银行应急制度建设与执行情况；

（二） 电子银行应急设施设备配备情况；

（三） 定期、持续性检测与演练情况；

（四） 应对意外事故或外部攻击的能力。

第三十四条 评估机构应制定本机构电子银行安全评定标准，在进行安全评估时，应根据委托机构的实际情况，确定不同评估内容对电子银行总体风险影响程度的权重，对每项评估内容进行评分，综合计算出被评估机构电子银行的风险等级。

第三十五条 评估完成后，评估机构应及时撰写评估报告，并于评估完成后 1 个月内向委托机构提交由其法定代表人或其授权委托人签字认可的评估报告。

第三十六条 评估报告应至少包括以下内容：

（一） 评估的时间、范围及其他协议中重要的约定；

（二） 评估的总体框架、程序、主要方法及主要评估人员介绍；

（三） 不同评估内容风险权重的确定标准，风险等级的计算方法，以及风险等级的定义；

（四） 评估内容与评估活动描述；

（五） 评估结论；

（六） 对被评估机构电子银行安全管理的建议；

（七） 其他需要说明的问题；

（八） 主要术语定义和所采用的国际或国内标准介绍（可作为附件）；

（九） 评估工作流程记录表（可作为附件）；

（十） 评估机构参加评估人员名单（可作为附件）。

在评估结论中，评估机构应采用量化的办法表明被评估机构电子银行的风险等级，说明被评估机构电子银行安全管理中存在的主要问题与隐患，并提出整改建议。

第三十七条　评估报告完成并提交委托机构后，如需修改，应将修改的原因、依据和修改意见作为附件附在原报告之后，不得直接修改原报告。

第四章　安全评估活动的管理

第三十八条　金融机构在申请开办电子银行业务时，应当按照有关规定对完成测试的电子银行系统进行安全评估。

第三十九条　金融机构开办电子银行业务后，有下列情形之一的，应立即组织安全评估：

（一） 由于安全漏洞导致系统被攻击瘫痪，修复运行的；

（二） 电子银行系统进行重大更新或升级后，出现系统意外停机 12 小时以上的；

（三） 电子银行关键设备与设施更换后，出现重大事故修复后仍不能保持连续不间断运行的；

（四） 基于电子银行安全管理需要立即评估的。

第四十条　金融机构对电子银行外部安全评估机构的选聘，应由金融机构的董事会或高级管理层负责。

第四十一条　已实现数据集中管理的银行业金融机构，其分支机构开展电子银行业务不需单独进行安全评估，在总行（公司）的电子银行安全评估中应包含对其分支机构电子银行安全管理状况的评估。

第四十二条　未实现数据集中管理的银行业金融机构，其分支机构开展电子银行业务且拥有独立的业务处理设备与系统的，分支机构的电子银行系统应在总行（公司）的统一管理和指导下，按照有关规定进行安全评估。

第四十三条　电子银行主要业务处理系统设置在境外的外资金融机构，其境外总行（公司）已经进行了安全评估且符合本指引有关规定的，其境内分支机构开展电子银行业务不需单独进行安全评估，但应按照本指引的有关要求，向监管部门报送安全评估报告。

第四十四条　电子银行主要业务处理系统设置在境内的外资金融机构，或者虽设置在境外但其境外总行（公司）未进行安全评估或安全评估不符合本指引有关规定的，应按规定开展电子银行安全评估工作。

第四十五条　电子银行安全评估工作，确需由多个评估机构共同承担或实施时，金融机构应确定一个主要的评估机构协调总体评估工作，负责总体评估报告的编制。

金融机构将电子银行系统委托给不同的评估机构进行安全评估，应当明确每个评估机构安全评估的范围，并保证全面覆盖了应评估的事项，没有遗漏。

第四十六条　金融机构应在签署评估协议后两周内，将评估机构简介、拟采用的评估方案和评估步骤等，报送中国银监会。

第四十七条　中国银监会根据监管工作的需要，可派员参加金融机构电子银行安全评估工作，但不作为正式评估人员，不提供评估意见。

第四十八条　评估机构应本着客观、公正、真实和自主的原则，开展评估活动，并严格保守在评估过程中获悉的商业机密。

第四十九条　在评估过程中，委托机构和评估机构之间应建立信息保密工作机制：

（一）评估过程中，调阅相关资料、复制相关文件或数据等，都应建立登记、签字制度；

（二）调阅的文件资料应在指定的场所阅读，不得带出指定场所；

（三）复制的文件或数据一般也不应带出工作场所，如确需带出的，必须详细登记带出文件或数据名称、数量、带出原因、文件与数据的最终处理方式、责任人等，并由相关负责人签字确认；

（四）评估过程中废弃的文件、材料和不再使用的数据，应立即予以销毁或删除；

（五）评估工作结束后，双方应就有关机密数据、资料等的交接情况签署说明。

第五十条　金融机构在收到评估机构评估报告的 1 个月内，应将评估报告报送中国银监会。

金融机构报送评估报告时，可对评估报告中的有关问题作必要的说明。

第五十一条　未经监管部门批准，电子银行安全评估报告不得作为广告宣传资料使用，也不得提供给除监管部门以外的第三方机构。

第五十二条　对未按有关要求进行的安全评估，或者评估程序、方法和评估报告存在重要缺陷的安全评估，中国银监会可以要求金融机构进行重新评估。

第五十三条　中国银监会根据监管工作的需要，可以自己组织或委托评估机构对金融机构的电子银行系统进行安全评估，金融机构应予以配合。

第五十四条　中国银监会根据监管工作的需要，可直接向评估机构了解其评估的方法、范围和程序等。

第五十五条　对于评估报告中所反映出的问题，金融机构应采取有效的措施加以纠正。

第五章　附则

第五十六条　本指引由中国银监会负责解释。

第五十七条　本指引自 2006 年 3 月 1 日起施行。

中国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

基本信息：	
【发布机关】中国人民银行	【时效性】现行有效
【发文字号】银发〔2011〕第 17 号	【效力级别】部门规范性文件
【发布日期】2011.01.24	【实施日期】2011.05.01

中国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

人民银行上海总部，各分行、营业管理部，各省会(首府)城市中心支行，国有商业银行，股份制商业银行，中国邮政储蓄银行：

个人金融信息是金融机构日常业务工作中积累的一项重要基础数据，也是金融机构客户个人隐私的重要内容。如何收集、使用、对外提供个人金融信息，既涉及到银行业金融机构业务的正常开展，也涉及客户信息、个人隐私的保护。如果出现与个人金融信息有关的不当行为，不但会直接侵害客户的合法权益，也会增加银行业金融机构的诉讼风险，加大运营成本。近年来，个人金融信息侵权行为时有发生，并引起社会的广泛关注。因此，强化个人金融信息保护和银行业金融机构法制意识，依法收集、使用和对外提供个人金融信息，十分必要。对个人金融信息的保护是银行业金融机构的一项法定义务。为了规范银行业金融机构收集、使用和对外提供个人金融信息行为，保护金融消费者合法权益，维护金融稳定，根据《中华人民共和国中国人民银行法》、《中华人民共和国商业银行法》、《中华人民共和国反洗钱法》、《个人存款账户实名制规定》等法律、法规的规定，现就个人金融信息保护的有关事项通知如下：

一、本通知所称个人金融信息，是指银行业金融机构在开展业务时，或通过接入中国人民银行征信系统、支付系统以及其他系统获取、加工和保存的以下个人信息：

(一)个人身份信息，包括个人姓名、性别、国籍、民族、身份证件种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等；

(二)个人财产信息，包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；

(三)个人账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等；

(四)个人信用信息，包括信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息；

(五)个人金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取、保存、留存的个人信息和客户在通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的个人信息等；

(六)衍生信息，包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；

(七)在与个人建立业务关系过程中获取、保存的其他个人信息。

二、银行业金融机构在收集、保存、使用、对外提供个人金融信息时，应当严格遵守法律规定，采取有效措施加强对个人金融信息保护，确保信息安全，防止信息泄露和滥用。特别是在收集个人金融信息时，应当遵循合法、合理原则，不得收集与业务无关的信息或采取不正当方式收集信息。

三、银行业金融机构应当建立健全内部控制制度，对易发生个人金融信息泄露的环节进行充分排查，明确规定各部门、岗位和人员的管理责任，加强个人金融信息管理的权限设置，形成相互监督、相互制约的管理机制，切实防止信息泄露或滥用事件的发生。

银行业金融机构要完善信息安全技术防范措施，确保个人金融信息在收集、传输、加工、保存、使用等环节中不被泄露。

银行业金融机构要加强对从业人员的培训，强化从业人员个人金融信息安全意识，防止从业人员非法使用、泄露、出售个人金融信息。接触个人金融信息岗位的从业人员在上岗前，应当书面做出保密承诺。

四、银行业金融机构不得篡改、违法使用个人金融信息。使用个人金融信息时，应当符合收集该信息的目的，并不得进行以下行为：

(一)出售个人金融信息；

(二)向本金融机构以外的其他机构和个人提供个人金融信息，但为个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定的除外；

(三)在个人提出反对的情况下，将个人金融信息用于产生该信息以外的本金融机构其他营销活动。

银行业金融机构通过格式条款取得客户书面授权或同意的，应当在协议中明确该授权或同意所适用的向他人提供个人金融信息的范围和具体情形。同时，还应当在协议的醒目

位置使用通俗易懂的语言明确提示该授权或同意的可能后果，并在客户签署协议时提醒其注意上述提示。

五、银行业金融机构不得将客户授权或同意其将个人信息用于营销、对外提供等作为与客户建立业务关系的先决条件，但该业务关系的性质决定需要预先做出相关授权或同意的除外。

六、在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

七、银行业金融机构通过外包开展业务的，应当充分审查、评估外包服务供应商保护个人金融信息的能力，并将其作为选择外包服务供应商的重要指标。

银行业金融机构与外包服务供应商签订服务协议时，应当明确其保护个人金融信息的职责和保密义务，并采取必要措施保证外包服务供应商履行上述职责和义务，确保个人金融信息安全。银行业金融机构应要求外包服务供应商在外包业务终止后，及时销毁因外包业务而获得的个人金融信息。

八、银行业金融机构通过接入中国人民银行征信系统、支付系统以及其他系统获取的个人金融信息，应当严格按照系统规定的用途使用，不得违反规定查询和滥用。

九、银行业金融机构发生个人金融信息泄露事件的，或银行业金融机构的上级机构发现下级机构有违反规定对外提供个人金融信息及其他违反本通知行为的，应当在事件发生之日或发现下级机构违规行为之日起 7个工作日内将相关情况及初步处理意见报告中国人民银行当地分支机构。

中国人民银行分支机构在收到银行业金融机构报告后，应视情况予以处理，并及时向中国人民银行报告。

十、中国人民银行及其地市中心支行以上分支机构受理投诉或发现银行业金融机构可能未履行个人金融信息保护义务的，可依法进行核实，认定银行业金融机构存在违反本通知规定，或存在其他未履行个人金融信息保护义务情形的，可采取以下处理措施：

(一)约见其高管人员谈话，要求说明情况；

(二)责令银行业金融机构限期整改；

(三)在金融系统内予以通报；

(四)建议银行业金融机构对直接负责的高级管理人员和其他直接责任人员依法给予处分；

(五)涉嫌犯罪的，依法移交司法机关处理。

十一、银行业金融机构违反规定通过中国人民银行征信系统、支付系统以及其他系统查询或滥用个人金融信息的，中国人民银行及其地市中心支行以上分支机构可按照本通知第十条及其他相关规定予以处理。

银行业金融机构违法情节严重或拒不改正的，中国人民银行可决定暂停其使用，或禁止其新设分支机构接入上述系统。

十二、银行业金融机构及其工作人员违反规定使用和对外提供个人金融信息，给客户造成损害的，应当依法承担相应的法律责任。

本通知自 2011 年 5 月 1 日起执行。请中国人民银行上海总部，各分行、营业管理部、省会 (首府)城市中心支行将本通知转发至辖区内各银行业金融机构。本通知执行过程中发现的新情况、新问题，请及时向中国人民银行报告。

中国人民银行

二 0一一年一月二十一日

最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知

基本信息：

【发布机关】最高人民法院，最高人民检察院，公安部

【发文字号】公通字[2013]12 号

【发布日期】2013.04.23

【时效性】 现行有效

【效力级别】部门规范性文件

【实施日期】2013.04.23

关于依法惩处侵害公民个人信息犯罪活动的通知

各省、自治区、直辖市高级人民法院，人民检察院，公安厅、局，新疆维吾尔自治区高级人民法院生产建设兵团分院，新疆生产建设兵团人民检察院、公安局：

近年来，随着我国经济快速发展和信息网络的广泛普及，侵害公民个人信息的违法犯罪日益突出，互联网上非法买卖公民个人信息泛滥，由此滋生的电信诈骗、网络诈骗、敲诈勒索、绑架和非法讨债等犯罪屡打不绝，社会危害严重，群众反响强烈。为有效遏制、惩治侵害公民个人信息犯罪，切实保障广大人民群众的个人信息安全和合法权益，促进社会协调发展，维护社会稳定，现就有关事项通知如下：

一、切实提高认识，坚决打击侵害公民个人信息犯罪活动。当前，一些犯罪分子为追求不法利益，利用互联网大肆倒卖公民个人信息，已逐渐形成庞大“地下产业”和黑色利益链。买卖的公民个人信息包括户籍、银行、电信开户资料等，涉及公民个人生活的方方

面面。部分国家机关和金融、电信、交通、教育、医疗以及物业公司、房产中介、保险、快递等企事业单位的一些工作人员，将在履行职责或者提供服务过程中获取的公民个人信息出售、非法提供给他人。获取信息的中间商在互联网上建立数据平台，大肆出售信息谋取暴利。非法调查公司根据这些信息从事非法讨债、诈骗和敲诈勒索等违法犯罪活动。此类犯罪不仅危害公民的信息安全，而且极易引发多种犯罪，成为电信诈骗、网络诈骗以及滋扰型“软暴力”等信息犯罪的根源，甚至与绑架、敲诈勒索、暴力追债等犯罪活动相结合，影响人们群众的安全感，威胁社会和谐稳定。各级公安机关、人民检察院、人民法院务必清醒认识此类犯罪的严重危害，以对党和人民高度负责的精神，统一思想，提高认识，精心组织，周密部署，依法惩处侵害公民个人信息犯罪活动。

二、正确适用法律，实现法律效果与社会效果的有机统一。侵害公民个人信息犯罪是新型犯罪，各级公安机关、人民检察院、人民法院要从切实保护公民个人信息安全和维护社会和谐稳定的高度，借鉴以往的成功判例，综合考虑出售、非法提供或非法获取个人信息的次数、数量、手段和牟利数额、造成的损害后果等因素，依法加大打击力度，确保取得良好的法律效果和社会效果。出售、非法提供公民个人信息罪的犯罪主体，除国家机关或金融、电信、交通、医疗单位的工作人员之外，还包括在履行职责或者提供服务过程中获得公民个人信息的商业、房地产业等服务业中其他企事业单位的工作人员。公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民个人隐私的信息、数据资料。对于在履行职责或者提供服务过程中，将获得的公民个人信息出售或者非法提供给他人，被他人用以实施犯罪，造成受害人人身伤害或者死亡，或者造成重大经济损失、恶劣社会影响的，或者出售、非法提供公民个人信息数量较大，或者违法所得数额较大的，均应当依法以非法出售、非法提供公民个人信息罪追究刑事责任。对于窃取或者以购买等方法非法获取公民个人信息数量较大，或者违法所得数额较大，或者造成其他严重后果的，应当依法以非法获取公民个人信息罪追究刑事责任。对使用非法获取的个人信息，实施其他犯罪行为，构成数罪的，应当依法予以并罚。单位实施侵害公民个人信息罪的，应当追究直接负责的主管人员和其他直接责任人员的刑事责任。要依法加大对财产刑的适用力度，剥夺犯罪分子非法获利和再次犯罪的资本。

三、加强协作配合，确保执法司法及时高效。侵害公民个人信息犯罪网络覆盖面大，关系错综复杂。犯罪行为发生地、犯罪结果发生地、犯罪分子所在地等往往不在一地。同时，由于犯罪行为大多依托互联网、移动电子设备，通过即时通讯工具、电子邮件等多种方式实施，调查取证难度很大、各级公安机关、人民检察院、人民法院要在分工负责、依法高效履行职责的基础上，进一步加强沟通协调，通力配合，密切协作，保证立案、侦查、

批捕、审查起诉、审判等各个环节顺利进行。对查获的及时立案侦查，及时移送审查起诉。对于几个公安机关都有权管辖的案件，由最初受理的公安机关管辖。必要时，可以由主要犯罪地的公安机关管辖。对管辖不明确或者有争议的刑事案件，可以由公安机关协商。协商不成的，由共同上级公安机关指定管辖。对于指定管辖的案件，需要逮捕犯罪嫌疑人的，由被指定管辖的公安机关提请同级人民检察院审查批准；需要提起公诉的，由该公安机关移送同级人民检察院审查决定；认为应当由上级人民检察院或者同级其他人民检察院起诉的，应当将案件移交有管辖权的人民检察院；人民检察院认为需要依照刑事诉讼法的规定指定审判管辖的，应当协商同级人民法院办理指定管辖有关事宜。在办理侵害公民个人信息犯罪案件的过程中，对于疑难、复杂案件，人民检察院可以适时派员会同公安机关共同就证据收集等方面进行研究和沟通协调。人民检察院对于公安机关提请批准逮捕、移送审查起诉的相关案件，符合批捕、起诉条件的，要依法尽快予以批捕、起诉；对于确需补充侦查的，要制作具体、详细的补充侦查提纲。人民法院要加强审判力量，准确定性，依法快审快结。

四、推进综合治理，建立防范、打击长效工作机制。预防和打击侵害公民个人信息犯罪是一项艰巨任务，必须标本兼治，积极探索和构建防范、打击的长效工作机制。各地公安机关、人民检察院、人民法院在依法惩处此类犯罪的同时，要积极参与综合治理，注意发现保护公民个人信息工作中的疏漏和隐患，及时通报相关部门，提醒和督促有关部门和单位加强监管、完善制度。要充分利用报纸、广播、电视、网络等多种媒体平台，大力宣传党和国家打击此类犯罪的决心和力度，宣传相关的政策和法律法规，提醒和教育广大群众运用法律保障和维护自身合法权益，提高自我防范的意识和能力。

给地接此通知后，请迅速传达至各级人民法院、人民检察院、公安机关。执行中遇到的问题，请及时报最高人民法院、最高人民检察院、公安部。

关于促进互联网金融健康发展的指导意见

基本信息：

【发布机关】中国人民银行、工业和信息化部、公安部、财政部、工商总局、法制办、银监会、证监会、保监会、国家互联网信息办公室

【发文字号】银发[2015]221 号

【发布日期】2015.07.14

【时效性】 现行有效

【效力级别】部门规范性文件

【实施日期】2015.07.14

关于促进互联网金融健康发展的指导意见【节选】

三、健全制度，规范互联网金融市场秩序

（十六）消费者权益保护。研究制定互联网金融消费者教育规划，及时发布维权提示。加强互联网金融产品合同内容、免责条款规定等与消费者利益相关的信息披露工作，依法监督处理经营者利用合同格式条款侵害消费者合法权益的违法、违规行为。构建在线争议解决、现场接待受理、监管部门受理投诉、第三方调解以及仲裁、诉讼等多元化纠纷解决机制。细化完善互联网金融个人信息保护的原则、标准和操作流程。严禁网络销售金融产品过程中的不实宣传、强制捆绑销售。人民银行、银监会、证监会、保监会会同有关行政执法部门，根据职责分工依法开展互联网金融领域消费者和投资者权益保护工作。

（十七）网络与信息安全。从业机构应当切实提升技术安全水平，妥善保管客户资料和交易信息，不得非法买卖、泄露客户个人信息。人民银行、银监会、证监会、保监会、工业和信息化部、公安部、国家互联网信息办公室分别负责对相关从业机构的网络与信息安全保障进行监管，并制定相关监管细则和技术安全标准。

国务院办公厅关于加强金融消费者权益保护工作的指导意见

基本信息：	
【发布机关】国务院办公厅	【时效性】 现行有效
【发文字号】国办发〔2015〕81 号	【效力级别】部门规范性文件
【发布日期】2015.11.04	【实施日期】2015.11.04

国务院办公厅关于加强金融消费者权益保护工作的指导意见

各省、自治区、直辖市人民政府，国务院各部委、各直属机构：

金融消费者是金融市场的重要参与者，也是金融业持续健康发展的推动者。加强金融消费者权益保护工作，是防范和化解金融风险的重要内容，对提升金融消费者信心、维护金融安全与稳定、促进社会公平正义和社会和谐具有积极意义。随着我国金融市场改革发展不断深化，金融产品与服务日趋丰富，在为金融消费者带来便利的同时，也存在提供金融产品与服务的行为不规范，金融消费纠纷频发，金融消费者权益保护意识不强、识别风险能力亟待提高等问题。为规范和引导金融机构提供金融产品和服务的行为，构建公平、公正的市场环境，加强金融消费者权益保护工作，经国务院同意，现提出如下意见：

一、指导思想

以党的十八大和十八届三中、四中、五中全会精神为指导，认真落实党中央、国务院决策部署，坚持市场化和法治化原则，坚持审慎监管与行为监管相结合，建立健全金融消

费者权益保护监管机制和保障机制，规范金融机构行为，培育公平竞争和诚信的市场环境，切实保护金融消费者合法权益，防范和化解金融风险，促进金融业持续健康发展。

二、工作要求

（一）人民银行、银监会、证监会、保监会（以下统称金融管理部门）要按照职责分工，密切配合，切实做好金融消费者权益保护工作。金融管理部门和地方人民政府要加强合作，探索建立中央和地方人民政府金融消费者权益保护协调机制。

（二）银行业机构、证券业机构、保险业机构以及其他从事金融或与金融相关业务的机构（以下统称金融机构）应当遵循平等自愿、诚实守信等原则，充分尊重并自觉保障金融消费者的财产安全权、知情权、自主选择权、公平交易权、依法求偿权、受教育权、受尊重权、信息安全权等基本权利，依法、合规开展经营活动。

（三）金融领域相关社会组织应当发挥自身优势，积极参与金融消费者权益保护工作，协助金融消费者依法维权，推动金融知识普及，在金融消费者权益保护中发挥重要作用。

三、规范金融机构行为

（一）健全金融消费者权益保护机制。金融机构应当将保护金融消费者合法权益纳入公司治理、企业文化建设和经营发展战略中统筹规划，落实人员配备和经费预算，完善金融消费者权益保护工作机制。

（二）建立金融消费者适当性制度。金融机构应当对金融产品和服务的风险及专业复杂程度进行评估并实施分级动态管理，完善金融消费者风险偏好、风险认知和风险承受能力测评制度，将合适的金融产品和服务提供给适当的金融消费者。

（三）保障金融消费者财产安全权。金融机构应当依法保障金融消费者在购买金融产品和接受金融服务过程中的财产安全。金融机构应当审慎经营，采取严格的内控措施和科学的技术监控手段，严格区分机构自身资产与客户资产，不得挪用、占用客户资金。

（四）保障金融消费者知情权。金融机构应当以通俗易懂的语言，及时、真实、准确、全面地向金融消费者披露可能影响其决策的信息，充分提示风险，不得发布夸大产品收益、掩饰产品风险等欺诈信息，不得作虚假或引人误解的宣传。

（五）保障金融消费者自主选择权。金融机构应当在法律法规和监管规定允许范围内，充分尊重金融消费者意愿，由消费者自主选择、自行决定是否购买金融产品或接受金融服务，不得强买强卖，不得违背金融消费者意愿搭售产品和服务，不得附加其他不合理条件，不得采用引人误解的手段诱使金融消费者购买其他产品。

（六）保障金融消费者公平交易权。金融机构不得设置违反公平原则的交易条件，在格式合同中不得加重金融消费者责任、限制或者排除金融消费者合法权利，不得限制金融消费者寻求法律救济途径，不得减轻、免除本机构损害金融消费者合法权益应当承担的民事责任。

（七）保障金融消费者依法求偿权。金融机构应当切实履行金融消费者投诉处理主体责任，在机构内部建立多层级投诉处理机制，完善投诉处理程序，建立投诉办理情况查询系统，提高金融消费者投诉处理质量和效率，接受社会监督。

（八）保障金融消费者受教育权。金融机构应当进一步强化金融消费者教育，积极组织或参与金融知识普及活动，开展广泛、持续的日常性金融消费者教育，帮助金融消费者提高对金融产品和服务的认知能力及自我保护能力，提升金融消费者金融素养和诚实守信意识。

（九）保障金融消费者受尊重权。金融机构应当尊重金融消费者的人格尊严和民族风俗习惯，不得因金融消费者性别、年龄、种族、民族或国籍等不同进行歧视性差别对待。

（十）保障金融消费者信息安全权。金融机构应当采取有效措施加强对第三方合作机构的管理，明确双方权利义务关系，严格防控金融消费者信息泄露风险，保障金融消费者信息安全。

四、完善监督管理机制

（一）完善金融消费者权益保护法律法规和规章制度。金融管理部门要推动及时修订与金融消费者权益保护相关的行政法规，积极推进金融消费者权益保护相关立法的基础性工作，研究探索金融消费者权益保护特别立法；逐步建立完善金融消费者权益保护规章制度，明确监管目标、原则、标准、措施和程序，指导建立金融消费者权益保护业务标准。

（二）加强金融消费者权益保护监督管理。金融管理部门要促进审慎监管与行为监管形成合力，依法加强监督检查，及时查处侵害金融消费者合法权益的行为；创新非现场监管方式，合理运用评估等手段，进一步提高非现场监管有效性；建立健全金融消费者投诉处理机制，有效督办、处理金融消费者投诉案件；完善风险提示和信息披露机制，加强创新型金融产品风险识别、监测和预警，防范风险扩散，加大对非法金融活动的惩处力度，维护金融市场有序运行。

（三）健全金融消费者权益保护工作机制。金融管理部门要健全机构设置，强化责任落实和人员保障；加强金融消费者权益保护协调机制建设，建立跨领域的金融消费者教育、金融消费争议处理和监管执法合作机制，加强信息共享，协调解决金融消费者权益保护领域的重大问题，形成监管合力；强化国际监管合作与交流，推动金融消费者权益跨境监管和保护。

（四）促进金融市场公平竞争。金融管理部门要有效运用市场约束手段防止金融机构不正当竞争行为，鼓励金融机构以提高客户满意度为中心开发更多适应金融消费者需要的金融产品和服务，提升服务水平，公平参与市场竞争。

五、建立健全保障机制

（一）提升金融消费者权益保护水平。有关部门和地方人民政府要在各自职责范围内

积极支持和配合金融消费者权益保护工作，健全全方位、多领域的金融消费者权益保护工作保障机制，依法打击各类金融违法犯罪活动，有效保护金融消费者合法权益。

（二）建立重大突发事件协作机制。对于涉及金融消费者权益保护的重大突发事件，地方人民政府负责协调本行政区域内各方力量做好应急处置工作。金融管理部门要积极协同配合，协调相关金融机构做好应急响应及处置工作。

（三）建立金融知识普及长效机制。金融管理部门、金融机构、相关社会组织要加强研究，综合运用多种方式，推动金融消费者宣传教育工作深入开展。教育部要将金融知识普及教育纳入国民教育体系，切实提高国民金融素养。

（四）建立金融消费纠纷多元化解决机制。金融管理部门、金融机构要建立和完善金融消费投诉处理机制，畅通投诉受理和处理渠道，建立金融消费纠纷第三方调解、仲裁机制，形成包括自行和解、外部调解、仲裁和诉讼在内的金融消费纠纷多元化解决机制，及时有效解决金融消费争议。

（五）促进普惠金融发展。金融管理部门要根据国家发展普惠金融有关要求，扩大普惠金融覆盖面，提高渗透率。金融机构应当重视金融消费者需求的多元性与差异性，积极支持欠发达地区和低收入群体等获得必要、及时的基本金融产品和服务。

（六）优化金融发展环境。建立以政府为主导、社会广泛参与的金融发展环境优化机制，加强社会信用体系建设，增强金融机构、金融消费者契约精神和信用意识，推动金融消费者权益保护环境评估工作，为保护金融消费者合法权益创造良好金融发展环境。

各地区、各有关部门要按照党中央、国务院决策部署，加强组织领导，注重沟通协调，强化组织和能力建设，在人力、财力、物力等方面给予充分支持。各有关部门要结合实际，抓紧研究制定具体实施办法，采取有效措施，切实承担起金融消费者权益保护监管职责，保护金融消费者合法权益，共同营造良好社会氛围，促进金融业持续健康发展，为实现全面建成小康社会的宏伟目标作出贡献。

国务院办公厅

2015 年 11 月 4 日

非银行支付机构网络支付业务管理办法

基本信息:	
【发布机关】中国人民银行	【时效性】 现行有效
【发文字号】中国人民银行公告[2015]第 43 号	【效力级别】部门规范性文件
	【实施日期】2016.07.01
【发布日期】2015.12.28	

非银行支付机构网络支付业务管理办法【节选】

第二章　客户管理

第六条　支付机构应当遵循“了解你的客户”原则，建立健全客户身份识别机制。支付机构为客户开立支付账户的，应当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，不得开立匿名、假名支付账户。

第三章 业务管理

第十一条　支付机构应根据客户身份对同一客户在本机构开立的所有支付账户进行关联管理，并按照下列要求对个人支付账户进行分类管理：

（一）对于以非面对面方式通过至少一个合法安全的外部渠道进行身份基本信息验证，且为首次在本机构开立支付账户的个人客户，支付机构可以为其开立Ⅰ类支付账户，账户余额仅可用于消费和转账，余额付款交易自账户开立起累计不超过 1000 元（包括支付账户向客户本人同名银行账户转账）；

（二）对于支付机构自主或委托合作机构以面对面方式核实身份的个人客户，或以非面对面方式通过至少三个合法安全的外部渠道进行身份基本信息多重交叉验证的个人客户，支付机构可以为其开立Ⅱ类支付账户，账户余额仅可用于消费和转账，其所有支付账户的余额付款交易年累计不超过 10 万元（不包括支付账户向客户本人同名银行账户转账）；

（三）对于支付机构自主或委托合作机构以面对面方式核实身份的个人客户，或以非面对面方式通过至少五个合法安全的外部渠道进行身份基本信息多重交叉验证的个人客户，支付机构可以为其开立Ⅲ类支付账户，账户余额可以用于消费、转账以及购买投资理财等金融类产品，其所有支付账户的余额付款交易年累计不超过 20 万元（不包括支付账户向客户本人同名银行账户转账）。

客户身份基本信息外部验证渠道包括但不限于政府部门数据库、商业银行信息系统、商业化数据库等。其中，通过商业银行验证个人客户身份基本信息的，应为Ⅰ类银行账户或信用卡。

第十四条　支付机构应当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，不得篡改或者隐匿交易信息。交易信息包括但不限于下列内容：

（一）交易渠道、交易终端或接口类型、交易类型、交易金额、交易时间，以及直接向客户提供商品或者服务的特约商户名称、编码和按照国家与金融行业标准设置的商户类别码；

（二）收付款客户名称，收付款支付账户账号或者银行账户的开户银行名称及账号；

（三）付款客户的身份验证和交易授权信息；

（四）有效追溯交易的标识；

（五）单位客户单笔超过 5 万元的转账业务的付款用途和事由。

第十六条　对于客户的网络支付业务操作行为，支付机构应当在确认客户身份及真实意愿后及时办理，并在操作生效之日起至少五年内，真实、完整保存操作记录。

客户操作行为包括但不限于登录和注销登录、身份识别和交易验证、变更身份信息和联系方式、调整业务功能、调整交易限额、变更资金收付方式，以及变更或挂失密码、数字证书、电子签名等。

客户操作行为包括但不限于登录和注销登录、身份识别和交易验证、变更身份信息和联系方式、调整业务功能、调整交易限额、变更资金收付方式，以及变更或挂失密码、数字证书、电子签名等。

第四章　风险管理与客户权益保护

第十七条　支付机构应当综合客户类型、身份核实方式、交易行为特征、资信状况等因素，建立客户风险评级管理制度和机制，并动态调整客户风险评级及相关风险控制措施。

支付机构应当根据客户风险评级、交易验证方式、交易渠道、交易终端或接口类型、交易类型、交易金额、交易时间、商户类别等因素，建立交易风险管理制度和交易监测系统，对疑似欺诈、套现、洗钱、非法融资、恐怖融资等交易，及时采取调查核实、延迟结算、终止服务等措施。

第二十条　支付机构应当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。

支付机构不得存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息，原则上不得存储银行卡有效期。因特殊业务需要，支付机构确需存储客户银行卡有效期的，应当取得客户和开户银行的授权，以加密形式存储。

支付机构应当以“最小化”原则采集、使用、存储和传输客户信息，并告知客户相关信息的使用目的和范围。支付机构不得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。

第二十一条　支付机构应当通过协议约定禁止特约商户存储客户银行卡的磁道信息或芯片信息、验证码、有效期、密码等敏感信息，并采取定期检查、技术监测等必要监督措施。

特约商户违反协议约定存储上述敏感信息的，支付机构应当立即暂停或者终止为其提供网络支付服务，采取有效措施删除敏感信息、防止信息泄露，并依法承担因相关信息泄露造成的损失和责任。

第二十二条　支付机构可以组合选用下列三类要素，对客户使用支付账户余额付款的交易进行验证：

（一）仅客户本人知悉的要素，如静态密码等；

（二）仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；

（三）客户本人生理特征要素，如指纹等。

支付机构应当确保采用的要素相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。

第二十三条　支付机构采用数字证书、电子签名作为验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、《金融电子认证规范》（JR/T0118-2015）等有关规定，确保数字证书的唯一性、完整性及交易的不可抵赖性。

支付机构采用一次性密码作为验证要素的，应当切实防范一次性密码获取端与支付指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内。

支付机构采用客户本人生理特征作为验证要素的，应当符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。

第五章　监督管理

第四十条　支付机构应当加入中国支付清算协会，接受行业自律组织管理。

中国支付清算协会应当根据本办法制定网络支付业务行业自律规范，建立自律审查机制，向中国人民银行备案后组织实施。自律规范应包括支付机构与客户签订协议的范本，明确协议应记载和不得记载事项，还应包括支付机构披露有关信息的具体内容和标准格式。

中国支付清算协会应当建立信用承诺制度，要求支付机构以标准格式向社会公开承诺依法合规开展网络支付业务、保障客户信息安全和资金安全、维护客户合法权益、如违法违规自愿接受约束和处罚。

第六章　法律责任

第四十一条　支付机构从事网络支付业务有下列情形之一的，中国人民银行及其分支机构依据《非金融机构支付服务管理办法》第四十二条的规定进行处理：

（一）未按规定建立客户实名制管理、支付账户开立与使用、差错争议和纠纷投诉处理、风险准备金和交易赔付、应急预案等管理制度的；

（二）未按规定建立客户风险评级管理、支付账户功能与限额管理、客户支付指令验

证管理、交易和信息安全管理、交易监测系统等风险控制机制的，未按规定对支付业务采取有效风险控制措施的；

（三）未按规定进行风险提示、公开披露相关信息的；

（四）未按规定履行报告义务的。

第四十二条　支付机构从事网络支付业务有下列情形之一的，中国人民银行及其分支机构依据《非金融机构支付服务管理办法》第四十三条的规定进行处理；情节严重的，中国人民银行及其分支机构依据《中华人民共和国中国人民银行法》第四十六条的规定进行处理：

（一）不符合支付机构支付业务系统设施有关要求的；

（二）不符合国家、金融行业标准和相关信息安全管理要求的，采用数字证书、电子签名不符合《中华人民共和国电子签名法》、《金融电子认证规范》等规定的；

（三）为非法交易、虚假交易提供支付服务，发现客户疑似或者涉嫌违法违规行为未按规定采取有效措施的；

（四）未按规定采取客户支付指令验证措施的；

（五）未真实、完整、准确反映网络支付交易信息，篡改或者隐匿交易信息的；

（六）未按规定处理客户信息，或者未履行客户信息保密义务，造成信息泄露隐患或者导致信息泄露的；

（七）妨碍客户自主选择支付服务提供主体或资金收付方式的；

（八）公开披露虚假信息的；

（九）违规开立支付账户，或擅自经营金融业务活动的。

第七章　附 则

第四十四条　本办法相关用语含义如下：

单位客户，是指接受支付机构支付服务的法人、其他组织或者个体工商户。

个人客户，是指接受支付机构支付服务的自然人。

单位客户的身份基本信息，包括客户的名称、地址、经营范围、统一社会信用代码或组织机构代码；可证明该客户依法设立或者可依法开展经营、社会活动的执照、证件或者文件的名称、号码和有效期限；法定代表人（负责人）或授权办理业务人员的姓名、有效身份证件的种类、号码和有效期限。

个人客户的身份基本信息，包括客户的姓名、国籍、性别、职业、住址、联系方式以

及客户有效身份证件的种类、号码和有效期限。

法人和其他组织客户的有效身份证件，是指政府有权机关颁发的能够证明其合法真实身份的证件或文件，包括但不限于营业执照、事业单位法人证书、税务登记证、组织机构代码证；个体工商户的有效身份证件，包括营业执照、经营者或授权经办人员的有效身份证件。

个人客户的有效身份证件，包括：在中国境内已登记常住户口的中国公民为居民身份证，不满十六周岁的，为居民身份证或户口簿；香港、澳门特别行政区居民为港澳居民往来内地通行证；台湾地区居民为台湾居民来往大陆通行证；定居国外的中国公民为中国护照；外国公民为护照或者外国人永久居留证（外国边民，按照边贸结算的有关规定办理）；法律、行政法规规定的其他身份证明文件。

客户本人，是指客户本单位（单位客户）或者本人（个人客户）。

中国人民银行关于进一步加强银行卡风险管理的通知

基本信息：	
【发布机关】中国人民银行	【时效性】 现行有效
【发文字号】银发[2016]170 号	【效力级别】部门规范性文件
【发布日期】2016.06.13	【实施日期】2016.06.13

中国人民银行关于进一步加强银行卡风险管理的通知【节选】

一、强化银行卡信息的安全管理

(一)强化支付敏感信息内控管理。各商业银行，支付机构 (从事银行卡收单业务，网络支付业务的非银行支付机构，下同)、银行卡清算机构应严格落实《中国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)，健全支付敏感信息安全内控管理制度，并将有关情况于 2016 年 9 月 1 日前报告人民银行。一是严禁留存非本机构的支付敏感信息(包括银行卡磁道或芯片信息、卡片验证码、卡片有效期、银行卡密码，网络支付交易密码等)，确有必要留有的应取得客户本人及账户管理机构的授权。二是明确相关岗位和人员的管理责任，严格分离不相容岗位并控制信息操作权限，制定信息操作流程和规范，强化内部监督、责任追究机制，严禁从业人员非法存储、窃取、泄露、买卖支付敏感信息。三是每年应至少开展两次支付敏感信息安全的内部审计，并形成报告存档备查，发现因系统漏洞造成支付敏感信息泄露或内部人员违规行为的，应立即采取有效措施防止风险扩大，并向人民银行报告；涉嫌违法犯罪的，应及时报告公安机关。

(二)加强支付敏感信息的安全防护。各商业银行，支付机构应在客户端软件与服务器、服务器与服务器之间进行通道加密和双向认证，对重要信息关键字段进行散列或加密存储，保障信息传输，存储、使用安全。开展网络支付业务时，不得委托或授权无支付业务资质的合作机构采集支付敏感信息，应采用具有信息输入安全防护、即时数据加密功能的安全控件，采取有效措施防止合作机构获取、留存支付敏感信息。

(三)全面应用支付标记化技术。自 2016 年 12 月 1 日起，各商业银行、支付机构应使用支付标记化技术(Tokenization)，对银行卡卡号、卡片验证码、支付机构支付账户等信息进行脱敏处理，并通过设置支付标记的交易次数、交易金额、有效期、支付渠道等域控属性，从源头控制信息泄露和欺诈交易风险。

(五)严格规范收单外包服务。各商业银行、支付机构应严格落实《银行卡收单业务管理办法》(中国人民银行公告[2013]第 9 号公布)、《中国人民银行关于加强银行卡收单业务外包管理的通知》(银发[2015]199 号)，承担收单环节支付敏感信息安全管理责任。一是不得将核心业务系统运营、受理终端密钥管理、特约商户资质审核等工作交由外包服务机构办理，二是指定专人管理终端密钥和相关参数，确保不同的受理终端使用不同的终端主密匙并定期更换。三是通过协议禁止实体和网络特约商户、外包服务机构留存支付敏感信息。四是每年对外包服务机构、实体和网络特约商户至少开展一次有一定独立性的安全评估，并形成报告存档备查，对于未遵守相关协议的，应立即中断合作。

二、加大银行卡互联网交易风险防控力度

（二）加强业务开通身份认证安全管理。自 2016 年 11 月 1 日起，各商业银行基于银行卡与支付机构、商业机构建立关联业务时，应严格采用多种因素身份认证方式，直接鉴别客户身份，并取得客户授权。身份鉴别应采取以下组合方式之一：一是采用复合《金融电子认证规范》（JR/T 0118）的数字证书，并组合交易密码等至少一种认证因素。二是采用复合《动态口令密码应用技术规范》（GM/T 0021）的动态令牌设备，并组合交易密码等至少一种认证因素。三是至少组合两种动态认证因素（如动态验证码、基于客户行为的动态挑战应答等），并采用语音、短信、数据（如手机银行、即时通讯、邮件）等至少两种不同通信渠道。

三、切实防范磁条卡伪卡欺诈交易风险

（三）加大特约商户实名制管理力度。银行卡清算机构应会同成员机构建立健全实体和网络特约商户信息电子化管理体系，严格落实特约商户实名制相关规定，完整、准确记录特约商户及其法定代表人或主要负责人的身份信息，并对同一特约商户在不同商业银行和支付机构注册的信息进行关联管理。充分利用影像采集、区域定位等技术，采取多渠道交叉验证等有限手段，健全特约商户资质审核和信息更新机制，持续加强特约商户信息真

实性管理。

（四）加强违规特约商户黑名单管理。一是各商业银行、支付机构应建立健全违规实体和网络特约商户黑名单管理制度，明确黑名单纳入与移出条件、惩罚措施等。加强对特约商户的监测、巡检，对于存在支付敏感信息泄露、非法改装终端、参与伪卡欺诈等违规行为的，应纳入黑名单管理，视严重程度从严采取延迟结算、暂停交易、终止合作等惩戒措施，并及时通知中国支付清算协会、银行卡清算机构。二是中国支付清算协会、银行卡清算机构应会同商业银行、支付机构建立健全黑名单信息共享和查询机制，加大联合惩戒力度，禁止拓展已纳入黑名单的特约商户。

四、严格落实各项规定，加大督查处罚力度

（一）严格落实国家网络安全和标准符合相关规定。各商业银行、支付机构、银行卡清算机构要严格落实国家网络安全和信息技术安全有关规定，使用经国家密码管理机构认可的商业密码产品。一是涉及的客户端软件、受理终端、银行卡、数字证书、动态令牌设备等应符合国家和金融行业相关标准，并通过国家认证认可管理部门认可机构的安全评估。二是业务系统建设和运营应符合国家信息安全等级保护的相关要求。三是业务系统及备份系统应按照国家网络安全相关要求部署在我国境内。

（二）建立健全监督检查机制。人民银行分支机构要高度重视、长抓不懈，成立银行卡风险管理领导小组，建立日常监督检查机制，将支付业务系统安全生产、受理终端（含网络支付接口）安全、支付敏感信息保护等纳入执法检查，统筹做好指导协调、政策宣传、执法检查、情况通报等工作。

（三）加大违规行为处罚力度。人民银行分支机构要严查因银行卡受理终端改装、支付交易验证强度低、系统存在安全漏洞及收到网络攻击等造成的支付服务中断、支付敏感信息泄露、资金损失事件，并依照《银行卡收单业务管理办法》、《非银行支付机构网络支付业务管理办法》等有关规定从严处罚。对于情节严重的，依照《中华人民共和国中国人民银行法》第四十六条规定，对相关机构及负有直接责任的董事、高级管理人员和其他直接责任人员进行处罚；涉嫌犯罪的，及时报告公安机关。对于情节严重的支付机构，还应按照《非金融机构支付服务管理办法》（中国人民银行令[2010]第 2 号发布）、《非银行支付机构分类评级管理办法》（银发[2016]106 号文印发）规定调低分类评级直至注销《支付业务许可证》。

网络借贷资金存管业务指引

基本信息：

【发布机关】中国银行业监督管理委员会(已撤销)　【时效性】 现行有效

【发文字号】银监办发[2017]21 号　【效力级别】部门规范性文件

【发布日期】2017.02.22　【实施日期】2017.02.22

网络借贷资金存管业务指引【节选】

第二章　委托人

第九条　在网络借贷资金存管业务中，委托人应履行以下职责：

（一）负责网络借贷平台技术系统的持续开发及安全运营；

（二）组织实施网络借贷信息中介机构信息披露工作，包括但不限于委托人基本信息、借贷项目信息、借款人基本信息及经营情况、各参与方信息等应向存管人充分披露的信息；

（三）每日与存管人进行账务核对，确保系统数据的准确性；

（四）妥善保管网络借贷资金存管业务活动的记录、账册、报表等相关资料，相关纸质或电子介质信息应当自借贷合同到期后保存 5 年以上；

（五）组织对客户资金存管账户的独立审计并向客户公开审计结果；

（六）履行并配合存管人履行反洗钱义务；

（七）法律、行政法规、规章及其他规范性文件和网络借贷资金存管合同（以下简称存管合同）约定的其他职责。

中国人民银行办公厅关于加强条码支付安全管理的通知

基本信息：

【发布机关】中国人民银行办公厅　【时效性】现行有效

【发文字号】银办发〔2017〕第 242 号　【效力级别】部门规范性文件

【发布日期】2017.12.22　【实施日期】2017.12.22

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)

中国人民银行上海总部，各分行、营业管理部，各省会(首府)城市中心支行，各副省级城市中心支行；各国有商业银行、股份制商业银行，中国邮政储蓄银行；中国银联股份有限

公司，中国支付清算协会，中国互联网金融协会，网联清算有限公司；各非银行支付机构：

为加强条码支付安全管理，切实保障人民群众财产安全和合法权益，现将《条码支付安全技术规范(试行)》(见附件 1)和《条码支付受理终端技术规范(试行)》(见附件 2)印发给你们，并提出如下工作要求，请一并遵照执行：

一、强化条码支付技术风险防范

各商业银行、非银行支付机构、清算机构要严格落实《条码支付安全技术规范(试行)》，强化条码支付技术风险防范。一是采取安全单元(SE)、支付标记化(Tokenization)、有效期控制、条码防伪识别等手段，保障条码的可靠性和有效性。二是运用交易验证强度与交易额度相匹配的技术措施提高条码支付交易的安全性。三是合理应用大数据分析、用户行为建模等手段建立条码支付风险监控机制，强化条码支付交易风险监测与预警。四是从木马病毒防范、信息加密保护、运行环境可信等方面提升条码支付客户端软件的安全防护能力。

二、推进条码支付受理终端注册管理

各商业银行、非银行支付机构、清算机构要严格落实《条码支付受理终端技术规范(试行)》，加强条码支付受理终端(含扫码设备、显码设备等)技术管理。清算机构应于 2018 年 1 月 31 日前完成条码支付受理终端注册管理、大数据分析校验等平台建设，并启动受理终端注册相关工作。各商业银行、非银行支付机构应积极配合清算机构做好受理终端注册等工作。

三、规范条码支付交易报文管理

各商业银行、非银行支付机构、清算机构要严格落实《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)要求，加强条码支付交易报文管理。一是采用数字签名、加密传输等措施，加强对支付指令真实性管理，防范交易信息被篡改或隐匿。二是在交易报文中准确记录发起方、接收方、网络路由等信息，采用唯一交易流水号、受理终端编码等，保障资金的可追溯性和支付指令的一致性。三是完善付款方、商户、渠道、订单等方面交易信息，精准刻画交易全貌，确保支付指令的完整性。

四、加强条码支付产品质量管理

各商业银行、非银行支付机构、清算机构、行业协会要严格落实《中国人民银行 国家认证认可监督管理委员会关于加强支付技术产品标准实施与安全管理的通知》(银发[2017]208 号)要求，加强标准落地实施，强化条码支付产品质量和安全管理，健全条码支付风险防控机制，有效提升条码支付产品的技术标准符合性和安全性。

五、加大督导管理力度

人民银行分支机构要统筹做好指导协调、政策宣传、情况通报等工作，对辖区内条码支付技术标准的落地实施情况进行监督，加大条码支付技术管理力度。行业协会要加强条码支付技术风险自律管理，定期向人民银行报送相关情况。

请人民银行上海总部，各分行、营业管理部，各省会(首府)城市中心支行，各副省级城市中心支行及时将本通知转发至辖区内各城市商业银行、农村商业银行、农村合作银行、民营银行、村镇银行、城市信用社、农村信用社和外资银行，加强组织落实

执行中如遇问题，请及时向人民银行报告。

联系人：张宏基　汤沁莹

联系电话：010-66194677　010-66194650

附件：1．条码支付安全技术规范(试行)

2．条码支付受理终端技术规范(试行)

中国人民银行办公厅

2017 年 12 月 22 日

附件 1

条码支付安全技术规范(试行)

2017 年 12 月

目次

1　范围

本规范规定了条码支付系统、终端、数据和交易的安全技术要求。

本规范适用于银行、非银行支付机构、清算机构开展条码支付业务时所需软硬件的设计、研发、集成和维护。

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／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 0118--2015　金融电子认证规范

JR／T 0149--2016　中国金融移动支付　支付标记化技术规范

条码支付受理终端技术规范(试行)

3　术语和定义

下列术语和定义适用于本文件。

3．1　条码　bar code

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。

3．2　线性条码　linear bar code

一维条码　one-dimensional bar code

条形码　bar code

宽度不等的多个熙条和空白，按照一定的编码规则排列，用以表达一组信息的图形标识符。

3．3　二维条码 two-dimensional bar code

二维码 two-dimensional bar code

在线性条码的基础上扩展出另一维具有可读性的条码，使用具有明显色差的深浅色矩形图案表示二进制数据，被设备识读和解码后可获取其中所包含的信息。

3．4　静态条码 static bar code

具有较长时效，可多次重复使用的条码。

3．5　动态条码　dynamic bar code

通过显码设备展示，并且有较短时效的条码。

3．6　条码支付　bar code payment

条码技术在支付领域中的应用，其本质是以条码为信息载体，通过移动终端或受理终端直接或间接获取支付要素，并利用已有支付渠道完成交易的一种支付方式。

3．7　移动终端 mobile terminal

具有移动通讯、条码展示或识读能力的客户设备，如手机、平板电脑等。

3．8　受理终端 payment torminal

具有条码展示或识读等功能，参与条码支付的商户端专用机具，包括显码设备和扫码设备。

3．9　显码设备 bat code display device

具有条码展示功能的专用设备。

3．10　扫码设备 bar code reader

识读条码并且向后台系统发起支付指令的专用设备，包括但不限于带扫码装置的收银机、POS 终端、自助终端等。

4　系统安全

4．1　物理安全要求

物理安全应符合 GB / T 22239--2008 中 7．1．1 的相关要求。

4．2　网络安全要求

网络安全应符合 GB / T 22239--2008 中 7．1．2 的相关要求。

4．3　主机安全要求

主机安全应符合 GB / T 22239--2008 中 7．1．3 的相关要求。

4．4　应用安全要求

4．4．1　基本要求

应用安全应符合 GB / T 22239--2008 中 7．1．4 的相关要求。

其他基本要求如下：

--不应在日志中记录客户支付敏感信息；

--应采用数字签名等技术手段保证交易信息的完整性；

--基于浏览器的应用，应使用数字证书标识网站身份，使用即时加密等安全措施降低恶意软件窃

取客户支付敏感信息的风险。

4．4．2　会话安全

会话安全要求如下：

--会话标识应唯一、随机、不可猜测：

--会话过程中应维持登录认证状态，防止信息未经授权访问；

--会话应设置超时时间，当空闲时间超过设定时间应自动终止会话；

--会话结束后，应及时清除会话信息；

--应采取加密等措施防止会话令牌在传输、存储过程中被窃取；

--应用审计日志宜记录暴力破解会话令牌的事件。

4．4．3　常见攻击防范

应对常见的攻击(如跨站脚本攻击、注入攻击、拒绝服务攻击等)进行有效防范，包括但不限于以下手段；

--应在服务器端对提交的数据进行有效性检查(如对提交的表单、参数等进行合法性判断和非法字符过滤等)；

--应对条码中包含的网址等信息进行校验，对非法地址和恶意请求进行拦截；

--应具有防范暴力破解的保护措施；

--应进行代码审查，防范应用程序中不可信数据被解析为命令或查询语句；

--应使用安全的接口，防范接口被攻击和非授权调用；

--应采取有效措施防范针对服务器端的拒绝服务攻击；

--应对文件的上传和下载进行访问控制，避免执行恶意文件或未授权访问；

--数据库宜使用存储过程或参数化查询，并严格定义数据库用户的角色和权限；

--宜通过自动化工具(如弱点扫描工具等)对应用程序进行检查。

4．5　数据安全及备份恢复

数据安全及备份恢复应符合 GB / T 22239--2008 中 7．1．5 的相关要求。

5　移动终端安全

5．1　人机交互安全

5．1．1　身份验证信息管理

身份验证信息管理应满足以下要求；

--原始身份验证信息不应明文保存在移动终端本地；

--客户输入交易密码时，应提供即时加密功能；

--验证操作结束后应及时清除缓存，防止信息泄漏；

--应严格限制使用初始交易密码，对交易密码复杂度进行校验，避免采用简单交易密码或与客户个人信息相似度过高的交易密码；

--应采取有效措施提醒客户避免设置与常用软件(如社交软件)、网站(如社交平台、论坛)相同或相似的用户名和密码组合；

--应采取有效措施引导客户设置独立的支付密码。

5．1．2　交易异常处理

当交易出现异常时，客户端应向客户提示出错等信息。

5．2　客户端软件安全

5．2．1　数据有效性校验

客户端软件应提供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应不含特殊字符、负数等非法参数。

5．2．2　页面回退清除敏感信息机制

客户端软件应支持页面回退清除密钥、密码等敏感信息的机制。

5．2．3　反编译

客户端软件应采用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。

5．2．4 客户端软件完整性

客户端软件完整性应满足以下要求：

--应对客户端软件进行签名，标识客户端软件的来源和发布者，保证客户所下载的客户端软件来源于所信任的机构；

--客户端软件启动和更新时，应进行真实性和完整性校验，防范客户端软件被篡改。

5．2．5 运行时安全

客户端软件运行时安全应满足以下要求：

--客户端软件应从木马病毒防范、信息加密保护、运行环境可信等方面提升安全防控能力；

--客户端软件应能监测并向后台系统反馈手机支付环境安全状况，作为风控策略的依据。

5．3　通信安全

5．3．1　网络通讯协议

网络通讯协议应满足以下要求：

--应在客户端与服务器之间建立安全的信息传输通道，通过公开网络进行数据传输时应进行双向认证，例如使用安全套接字层或传输层安全(SSL／TLS)、互联网协议安全(IPSec)等协议；

--如果使用 SSL／TLS 协议，应使用安全的版本，取消对存在安全隐患版本协议的支持。

5．3，2　抗抵赖

通过客户端发送报文的关键要素宜进行数字签名，以确保支付内容的真实性和抗抵赖性。

6　受理终端安全

受理终端安全应满足以下要求：

--参照《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)等相关要求，应从终端产品选型、验收、现场检查等环节加强安全管理，确保终端的技术标准符合性；

--受理终端应使用经国家密码管理机构认可的商用密码产品；

--应符合《条码支付受理终端技术规范(试行)》相关要求。

7　交易安全

7．1　基本要求

交易安全应满足以下要求：

--应遵守国家安全、国家网络安全相关法律法规，严格落实《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)等相关规定，确保条码支付业务设施的安全、稳定和高效运行；

--应按照了 JR／T0149 的相关要求，对银行卡卡号、卡片验证码、支付账户等信息进行脱敏，支持基于支付标记化技术的交易处理，采取技术手段从源头控制信息泄露和欺诈交易风险；

--条码支付涉及的软硬件应使用经国家密码管理机构认可的商用密码产品；

--应定期开展支付敏感信息安全的内部审计；

--支付敏感信息的采集、存储，传输、使用等环节应符合《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)的要求。

7．2　码制

条码应使用符合国家标准的码制。

7．3　数据录入

数据录入应满足以下要求：

--客户输入交易密码等信息，客户端不应明文显示；

--客户输入支付敏感信息时，应采用信息输入安全防护、即时数据加密等安全措施防止数据被非法截获；

--客户输入支付敏感信息时，应采取防篡改机制防止数据被非法篡改；

--客户输入关键交易信息时，如收款人信息、交易金额等，应采取防篡改机制防止数据被非法篡改。

7．4　数据访问

数据访问应满足以下要求：

--应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；

--支付敏感信息应按业务需求进行保存和使用，显示时应进行屏蔽处理。

7．5　数据存储

数据存储应满足以下要求：

--在满足法律、管理规定的前提下，客户端应保留最少的客户信息，并限制数据存储量和保留时间；

--客户端在使用支付敏感信息后，应及时清除；

--不得留存非本机构的支付敏感信息，确有必要留存的，应取得客户本人及账户管理机构的授权

并进行加密或不可逆变换。

7．6　数据传输

数据传输应满足以下要求；

--支付敏感信息通过公共网络传输时应采取加密措施，保证支付敏感信息传输的保密

性；

--支付敏感信息在本地软件其他进程间传输时应采取加密措施，保证支付敏感信息传输的保密性；

--交易信息在传输时，客户端应采取安全措施如报文鉴别码(MAC)以确保交易信息的完整性。

7．7　条码生成

7．7．1　基本要求

条码支付分为收款扫码和付款扫码。收款扫码是指收款人通过识读付款人移动终端展示的条码完成支付的行为。付款扫码是指付款人通过移动终端识读收款人展示的条码完成支付的行为。

条码生成时，应满足以下基本要求：

--应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；

--应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；

--应根据风控能力，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。

7．7．2　收款扫码

收款扫码的条码生成方式包括服器端生成条码和移动终端生成条码两大类。其中，服务器端生成条码方式包括移动终端实时获取、移动终端批量获取：移动终端生成条码方式包括安全单元(SE)加密动态生成、客户端软件通过生成因子加密动态生成。

采用收款扫码方式时，应满足以下基本要求：

--展示条码的客户端应先进行身份验证；

--条码应限制一次使用且展示周期原则上应小于 1 分钟；

--应采取有效措施防止展示条码被截屏等方式窃取；

--应采用加密方式生成条码。

对于服务器端生成、由移动终端批量获取的条码生成方式，还应满足以下要求：

--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，应以安全的方式在移动终端上保存；

--保存的条码应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；

--预生成的条码应定期更换，更新周期宜小于 24 小时；

--应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，后台服务器应对客户端软件进行身份验证，防止恶意获取条码。

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，还应满足以下要求：

--移动终端客户端软件应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；

--条码生成因子应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；

--条码生成因子应定期更换，更新周期宜小于 7 天；

--应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。

7．7．3　付款扫码

采用付款扫码方式时，条码生成应满足以下要求：

--采用显码设备展示条码时：

·条码应加密、动态生成，原则上应实时生成或从后台服务器获取，并限一次性使用。

--采用静态条码时：

·条码应由后台服务器加密生成；

·宜采用防伪纸张展示条码，可参考附录 A；

·展示条码的介质应放置在商户收银员视线范围内，并采用防护罩等物理防护手段避免条码被覆盖或替换，商户应定期对介质进行检查；宜使用防伪封签对防护罩等物理防护手段进行标记，及时发现物理防护手段被人为破坏，可参考附录 A；

·应在介质显著位置明显展示收款人信息，便于客户核对信息。

7．8　条码识读与解析

条码识读设备应保证识读结果的保密性，避免条码信息泄露。

条码解析时应满足以下要求：

--应对条码的完整性进行校验；

--应对条码的真实性进行校验；

--应保证条码解析程序自身的健壮性；

--应识别病毒、木马等恶意代码，保障交易的安全性。

7．9　交易验证与确认

交易验证可以组合选用下列三类要素：

--仅客户本人知悉的要素，如静态密码等；

--仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；

--客户本人生物特征要素，如指纹等。

交易验证要素的使用，应满足以下要求：

--应确保采用的要素相互独立，即部分要素的损坏或者泄露不应导致其他要素损坏或者泄露；

--采用数字证书、电子签名作为验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》、JR / T 0118 等有关规定，确保数字证书的唯一性、完整性及交易的抗抵赖性；

--采用一次性密码作为验证要素的，应切实防范一次性密码获取端与支付指令发起端为相同物理设备而带来的风险，并将一次性密码有效期严格限制在最短的必要时间内；

--采用客户本人生物特征作为验证要素的，应符合国家、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。

采用付款扫码支付方式时，应满足以下要求；

--应在移动终端展现交易信息，并在界面的显著位置展示收款人信息，便于客户核对；

--应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施；

--由付款人发起支付指令，交易信息包含但不限于收款人名称、金额等。

采用收款扫码支付方式时，应满足以下要求：

--应经过客户确认并进行交易验证，交易验证宜同时采用上述三类要素中的两类要素，不足两类的应采取相应的风险补偿措施：

--在移动终端进行交易验证时，应在移动终端上展现交易信息。

7．10　交易风险控制

应采用大数据分析、客户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时预警，并采取调查核实、风险提示、延迟结算等处理措施。

针对批量或高频登录等异常行为，应利用 IP 地址、终端设备标识等信息进行综合识

别，及时采取附加验证、拒绝请求等手段。

对于资金类交易等高风险业务，应在确保客户联系方式有效的前提下，及时告知客户其资金变化情况。

应按照 7．9 条进行交易验证，根据不同风险防范能力设置相应的日累计交易限额。

使用动态条码进行支付的，风险防范能力分级见表 1。

表 1　风险防范能力分级表

交易验证方式	风险防范能力
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(具体要求见 7．9 条)。	A 级
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(具体要求见 7．9 条)。	B 级
采用不足两类有效要素进行验证的(具体要求见 7．9 条)。	C 级

使用静态条码进行支付的，风险防范能力为 D 级。

7．11　交易过程安全

7．11．1　交易报文安全

按照《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)等相关规定，交易报文安全应满足以下要求：

--应防止对交易的重放攻击；

--应保证交易的抗抵赖性，包括但不限于数字证书、电子签名等技术手段；

--在交易报文传输过程中应使用安全协议保证传输安全；

--应用系统应保证在一段时期内同一商户交易、订单的唯一性；

--应用系统应检查交易请求报文中记载的交易要素是否完整，拒绝不完整的交易请求；

--应用系统应防止对支付成功的订单重复支付；

--应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；

--应提供用户客户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户客户身份标识、身份鉴别信息不易被冒用。

7．11．2　风险识别与干预

风险识别与干预应满足以下要求；

--应采取必要措施，在交易过程中给予必要的支付风险提示，可每次提示，也可在业务开通时给予提示；

--应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。

7．11．3　交易监控

交易监控应满足以下要求：

--应建立交易监控系统，能够甄别并预警潜在风险的交易，例如套现、洗钱、欺诈等可疑交易，并生成风险监控报告；

--应根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、复核、查结机制；

--应对监控到的风险交易进行及时分析与处置；

--应建立条码支付的黑白名单验证和管理机制，在黑名单中的应直接拒绝。

7．11．4　客户和商户教育

客户和商户教育应满足以下要求：

--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；

--应在支付过程中向客户明确提示相关的安全风险和注意事项

--应加强对交易密码等信息的保护管理和客户安全教育，提示客户及时修改密码；

--应向商户提示静态条码的风险及防范措施。

附　录　A

(资料性附录)

防伪技术要求

A．1　概述

防伪纸张适用于通用打印机打印，主要用于打印静态条码，粘贴在商户经营场所内进行静态条码展示。

防伪封签单面可粘贴，粘贴后不易脱落，主要用于静态条码展示介质物理防护手段的标记。防伪封签贴在静态条码展示介质物理防护手段开口处，避免后期人为替换静态条码。

防伪纸张和防伪封签采用特种印刷工艺生产，具有易识别、防复制、难伪造、可追溯的特点，便于长期使用和识别。

A．2　防伪技术

防伪纸张的材质为特种防伪纸，防伪封签的材质为特种防伪不干胶纸，应采用防伪技术，具备多种防伪特征，如炫彩动感光变开窗安全线、光彩光变图案、雕刻凹印图案、环形光角变色纤维、有色荧光图案、有色荧光号码等。

A．3　技术要求

A．3．1　规格

防伪纸张宜为矩形，方便打印，中间预留方形静态条码打印区域。

防伪纸张克重宜为 100g / ㎡ ~ 120g / ㎡。

防伪封签克重(面纸加底纸)宜为 120g / ㎡ ~ 160g / ㎡。

A．3．2 外观质量

表面平整光洁，不得有破损、残缺、卷边、多边、卷角、荷叶边等。

文字图案线条清晰，墨色适当，无模糊、浅花、断线、蹭脏等问题。

开窗安全线开窗规整，不得出现无线、乱线、多根线、翻面线、子母线等。

A．3．3 荧光特征

防伪纸张和防伪封签的荧光特征明显、图案完整、颜色鲜明。

A．3．4 物化耐性

防伪纸张和防伪封签应具有较强的耐酸、耐碱、耐热水、耐光等特性。

参考文献

[1]GB / T 12406--2008　表示货币和资金的代码

[2]GB / T 22080--2016　信息技术　安全技术　信息安全管理体系　要求

[3]GB / T 22081--2016　信息技术　安全技术　信息安全控制实践指南

附件 2

条码支付受理终端技术规范

(试行)

2017 年 12 月

目次

1　范围

本规范规定了条码支付涉及到的受理终端在展示、识读、安全保护、适应性和可靠性方面的技术要求。

本规范适用于银行、非银行支付机构、清算机构开展条码支付业务时所需受理终端的设计、研发、维护和采购。

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 23704--2009　信息技术　自动识别与数据采集技术　二维条码符号印制质量的检验

JR / T 0120．1　银行卡受理终端安全规范　第 1 部分，销售点(POS)终端

JR / T 0120．2　银行卡受理终端安全规范　第 2 部分，受理商户信息系统

JR / T 0120．5　银行卡受理终端安全规范　第 5 部分：PIN 输入设备

3　术语和定义

下列术语和定义适用于本文件。

3．1　条码　bar code

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。

3．2　线性条码 linear bar code

一维条码 one-dimensional bar code

条形码 bar code

宽度不等的多个黑条和空白，按照一定的编码规则排列，用以表达一组信息的图形标识符。

3．3　二维条码 two-dimensicnal bar code

二维码 two-dimensional code

在线性条码的基础上扩展出另一维具有可读性的条码，使用具有明显色差的深浅色矩形图案表示二进制数据，被设备识读和解码后可获取其中所包含的信息。

3．4　条码支付　bar code payment

条码技术在支付领域中的应用，其本质是以条码为信息载体，通过移动终端或受理终端直接或间接获取支付要素，并利用已有支付渠道完成交易的一种支付方式。

3．5　受理终端 payment terminal

具有条码展示或识读等功能，参与条码支付的商户端专用机具，包括显码设备和扫码设备。

3．6　显码设备 bar code display device

具有条码展示功能的专用设备。

3．7　扫码设备 bar code reader

识读条码并且向后台系统发起支付指令的专用设备，包括但不限于带扫码装置的收银机、POS 终端、自助终端等。

3．8　移动终端　mobile terminal

具有移动通讯、条码展示或识读能力的客户设备，如手机、平板电脑等。

3．9　打印对比度 print contrast signal

码图(条码符号)中浅色模块反射率(用 Rmax 表示)、深色模块反射率(用 Rmin 表示)之差与浅色模块反射率的百分比，用 PCS 表示。

计算公式：PCS = [(Rmax-Rmin) / Rmax] × 100％

3．10　测试版 test chart

由各种码图样本及其它信息构成的测试卡片，包含标准测试版、打印对比度测试版、低品质测试版等。

3．11　标准测试版 standard test chart

由 GB / T23704--2009 中规定符号等级为“A”的码图样本组成，用于考察产品对标准条码的识读效果。

4　显码设备技术要求

4．1　数据要求

4．1．1　正确性

显码设备的数据正确性应满足以下要求：

--输入数据信息转成一个或多个条码，被识读解码后应完全重现输入数据信息，不得出现任何差异；

--条码的表达应符合相应的国家标准。输入数据信息转成一个或多个条码，被条码识读设备识读后的数据信息应具有唯一性。

4．1．2　规范性

显码设备的数据规范性应满足以下要求：

--输入数据信息，如果包含采用 GB 18030--2005 编码的汉字，且条码码制支持汉字编码类型，应优先采用汉字编码类型表述输入数据信息中的汉字；

--输入数据信息，如果能被条码码制用多种内部数据编码类型表述的，应优先采用最紧凑的数据编码类型表述。输入数据信息可以分段采用不同的内部数据编码类型，实现整体的紧凑表述；

--二维条码纠错等级应选用可恢复码字比例不小于 15%的等级；

--在满足上述条件基础上，二维条码应选用最小的符号版本。

4．1．3　码制

条码应使用符合国家标准的码制。

4．2　条码表现要求

4．2．1　外形

显码设备显示的条码外形应满足以下要求：

--应表现在平面介质上，不得扭曲、变形、破坏；

--应完整表现，且条码外围空白区应符合码制要求。

4．2．2　介质

条码可表现在以下介质上：

--主动发光表面介质，包括但不限于液晶显示器(LCD)、发光二极管(LED)屏幕等；

--半主动发光表面介质，包括但不限于光学投影幕墙等；

--被动反射表面介质，包括但不限于电子墨水屏幕等。

4．2．3　颜色

显码设备显示的条码颜色应满足以下要求：

--条码主体应采用黑白或深浅反差尽量大的两种色块表示；

--对于被动反射表面介质，要求 PCS 值不小于 30％。

4．2．4　精度

不同条码表现介质上的精度应满足以下要求：

--对于被动反射表面介质，最高表示精度不应超过 0．254mm(10mil)；

--对于主动、半主动发光表面介质，最高表示精度不应超过 0．381mm(15mil)。

5　扫码设备技术要求

5．1　数据要求

5．1．1　准确性

扫码设备识读条码应满足以下要求：

--条码支付交易过程一次识读后输出的数据信息，应具有唯一性和可重复性；

--条码的识读解码机制应符合相应的国家标准，输出数据信息的表达应没有歧义。

5．1．2　规范性

扫码设备识读条码后的输出数据信息如果包含汉字，汉字编码字符集应符合 GB 18030--2005 等。

5．2　性能要求

5．2．1　精度

扫码设备识读条码的精度应满足以下要求：

--对于被动反射表面介质，最高识读精度应达到 0．254mm(10mil)；

--对于主动、半主动发光表面介质，最高识读精度应达到 0．381mm(15mil)。

5．2．2　识读速度

扫码设备识读一个条码的时间应不超过 1 秒。

5．2．3　出错率

对于识读解码能力范围内的标准测试版，出错率应小于 0．01%。

6　安全性技术要求

条码支付受理终端应符合以下安全性技术要求：

--应保证条码识读结果的机密性，避免条码信息泄露。

--应保证条码解析的准确性。

--应保证条码识读解析结果表达的规范性。

--受理终端如果用于个人识别码(PIN)输入相关场景，应具备物理、逻辑安全机制，包括但不限于：

·应具备入侵检测机制；

·应防止 PIN 输入过程被监听；

·应保证支付敏感信息的安全存储；

·应具备完整的密钥体系；

·在 PIN 输入设备和非接触式读卡器间传输 PIN 相关信息时，应采取有效措施保护所传输的数据；

·PIN 输入设备应符合 JR / T 0120．5 的要求。

--在条码支付交易过程中，受理终端应符合 JR / T 0120．1、JR / T 0120．2 等相关要求；涉及支付敏感信息处理的还应符合《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)的要求。

--在条码支付交易过程中，受理终端需要输入身份验证信息的，应对身份验证信息的输入方式、过程及内容具备安全防护机制。

--受理终端应具有唯一标识，唯一标识应以安全方式保护，以保障无法被篡改，如使用安全单元 (SE)、可信执行环境(TEE)等；交易报文中应包含受理终端标识，并采取加密绰措施保证在交易过程中不可被篡改。

--应采取技术手段实现条码支付受理终端、通讯网络与商户自身业务系统的隔离。

--应在受理终端与服务器之间建立安全的信息传输通道，通过公开网络进行数据传输时应进行双向认证，例如使用安全套接字层或传输层安全(SSL / TLS)、互联网协议安全(IPSec)等协议；

如果使用 SSL / TLS 协议，应使用安全的版本，取消对存在安全隐患版本协议的支持。

7 适应性技术要求

7．1 电源适应能力

在额定电压偏差 ± 5% 范围内的条件下，受理终端应能正常工作。

7．2 接口

受理终端需要与外部进行数据传输交换的，应支持以下全部或部分类型的接口：

--串行通讯接口(RS232、RS485 等)；

--USB 接口；

--红外通讯接口；

--以太网通讯接口；

--蓝牙通讯接口；

--无线通讯接口；

--其他。

7．3 环境适应性

7．3．1 气候环境适应性

气候环境适应性应满足表 1 的要求。

表 1 气候环境适应性

设备状态	气候环境	
	温度	相对湿度
工 作	O℃ ~ 40℃	15%--90%，无冷凝
贮 存 运 输	-20℃ ~ 60℃	5%--93%，无冷凝

7．3．2 光照环境适应性

受理终端在不同光照环境下应满足以下要求：

--在户外阳光照射不高于 86112 Lux 的照度下应能正常工作；

--在室内不高于 4842 Lux 的照度下应能正常工作。

参考文献

[1]GB / T 5007．1--2010 信息技术 汉字编码字符集(基本集) 24 点阵字型

[2]GB / T 5199--2010　信息技术 汉字编码字符集(基本集)　15 × 16 点阵字型

[3]6B / T 9254--2008　信息技术设备的无线电骚扰限值和测量方法

[4]GB / T 13000--2010　信息技术 通用多八位编码字符集(UCS)

[S]GB / T 17618--2015　信息技术设备 抗扰度 限值和测量方法

[6]GB 17625．1--2012　电磁兼容 限值 谐波电流发射限值(设备每相输入电流≤16A)

中国人民银行关于进一步加强征信信息安全管理的通知

基本信息：	
【发布机关】中国人民银行	【时效性】现行有效
【发文字号】银发〔2018〕第 102 号	【效力级别】部门规范性文件
【发布日期】2018.04.25	【实施日期】2018.04.25

中国人民银行关于进一步加强征信信息安全管理的通知

中国人民银行上海总部，各分行、营业管理部，各省会(首府)城市中心支行，各副省级城市中心支行；国家开发银行，各政策性银行、国有商业银行、股份制商业银行，中国邮政储蓄银行：

为贯彻落实党的十九大精神和第五次全国金融工作会议精神，加强个人信息保护，做好新时代征信信息安全管理工作，切实保护信息主体合法权益，提升人民群众在征信领域的幸福感和安全感，依据《征信业管理条例》、《个人信用信息基础数据库管理暂行办法》(中国人民银行令[2005]第 3 号发布)等法规规章的相关规定，现就进一步加强金融信用信息基础数据库运行机构和接入机构(以下简称运行机构和接入机构)征信信息安全管理有关事项通知如下：

一、切实增强征信信息安全管理意识，强化征信信息安全主体责任

运行机构和接入机构要清醒认识当前征信信息安全面临的严峻形势，切实增强征信信息安全管理意识。建立健全征信信息安全管理的体制和机制，成立征信信息安全工作领导小组，明确岗位职责，强化征信信息安全主体责任，按照“分级管理、逐级负责”和“谁主管谁负责、谁使用谁负责”的原则，明确领导层中分管征信工作的负责人为第一责任人，征信系统及相关信息系统的使用人为直接责任人，并明确第一责任人、直接责任人和其他相关人员的责任分工。

二、完善征信业务操控流程，不断提高征信信息安全管理水平

运行机构和接入机构要切实加强对征信各级管理人员和从业人员的全员征信合规性教

育培训，围绕征信信息安全管理，通过加强征信系统用户管理、健全征信信息查询管理、优化自助查询机管理、完善征信异常查询监控机制、妥善办理异议与投诉等措施，完善征信业务操控流程，牢牢守住不发生征信信息安全风险的底线。

(一)从严加强征信系统用户管理。

运行机构和接入机构应严格遵循相关规定办理用户的创建、停用和启用，根据“最小授权”原则分配各类、各级用户的权限，严格用户权限设置，将用户权限控制在业务需要的最小范围内。杜绝创建公共账户或者类公共账户，切实做到人户统一、专人专用，及时停用和启用用户，实施用户密码动态管理。

运行机构和接入机构应不断更新技术保障措施，加强对各级征信系统用户运行情况的实时监控。分级负责，明确责任，技防和人防相结合，在制度措施保障上不留真空和死角。

(二)健全征信信息查询管理。

运行机构和接入机构要健全征信信息查询管理，严格授权查询机制，未经授权严禁查询征信报告，规范内部人员和国家机关查询办理流程，严禁未经授权认可的 APP 接入征信系统。从严管理批量数据，按照合法、正当、必要的原则，严格按流程和保密要求办理批量数据的抽取、留存、流转、应用和销毁，确保各环节数据安全。

(三)优化自助查询机管理。

运行机构和接入机构应优化自助查询机用户管理，明确自助查询机用户管理权限，及时停用或者删除无效用户；加强访问控制，为自助查询机单独划分网段，根据工作时间和查询需要，合理设置自助查询机自动关机时间；采购自助查询机时，完善合同内容，明确设备提供商的保密责任；健全自助查询机物理设备管理，明确自助查询机管理责任主体，对设备加强维护，按流程及时清理自助查询机内部存储的征信信息。

(四)完善征信异常查询监控机制，妥善办理异议与投诉。

运行机构和接入机构应分级建立征信用户查询操作日核查机制，完善异常查询监控、处置与报告机制；不断优化和调整征信查询日核查与实时监控指标，不断提高征信用户自查与自控的能力。严格遵守异议处理时间，规范异议处理流程，按规定出具相关文书，做好异议申请、处理资料的保存、归档；强化投诉办理，规范投诉流程，及时办理信息主体投诉，提高信息主体的满意度。以异议和投诉为重要线索，对可能涉及的征信信息安全风险事件及时进行全面排查，及时发现问题和排除隐患。

三、查漏补缺，补齐短板，完善征信内控制度及问责制度

运行机构和接入机构应结合自身实际对自身的征信内控制度及问责制度进行全面自建自查，查漏补缺，补齐短板，并重点从以下三个方面加以完善：

(一)建立征信内控制度及问责制度的报备制度。

自本通知发布之日起，运行机构和接入机构应在 30 个工作日内，向人民银行报备经本机构法定代表人或者主要负责人签字并加盖公章的征信合规与信息安全内控制度及问责制度。运行机构及全国性接入机构(名单见附件 1)的总行向人民银行征信管理局报备，地方性接入机构和全国性接入机构的分支机构向所在地人民银行分支机构报备。征信内控制度及问责制度变更的，应当自变更之日起 10 日内向人民银行报备。

(二)建立征信信息安全情况报告制度。

运行机构和接入机构应按月定期向人民银行报送异常查询、违规查询、非法提供、违规使用、信用报告泄漏等征信信息安全情况统计表(见附件 2)。未发生征信信息安全风险事件的，应采取零报告制度(即在表中填报“0”)。发生征信信息安全风险事件的，应立即上报相关情况。全国性接入机构的总行应于每月初 10 日内将上月情况报送人民银行征信管理局；地方性接入机构和全国性接入机构的分支机构应于每月初 6 日内将上月情况报所在地人民银行分支机构；人民银行副省级城市中心支行以上分支机构应于每月初 10 日内将汇总的辖区内上月情况(包括人民银行分支机构征信查询点情况)报送征信管理局。

(三)建立征信合规与信息安全自查自纠制度及报告制度。

运行机构和接入机构应建立分级监控、专项核查的工作机制，按照征信内控制度的规定，对日常监测发现的风险线索以及异常查询线索，与对应的信贷业务进行逐笔核实，从授权、审核、查询、使用、存储等各环节梳理是否存在征信违规风险隐患，不定期组织抽查，建立健全征信合规与信息安全自查自纠制度，并向人民银行报备，报备流程参照征信内控制度及问责制度的报备要求。按季度开展内部征信合规和信息安全自查自纠，并将自查自纠情况向人民银行书面报告，报告流程参照征信信息安全事件的报告要求。

四、提高技防能力，防范征信信息泄露风险

运行机构和接入机构应不断优化升级征信业务信息系统，提升前置自控能力，推进业务触发式查询，实现信用报告脱敏展示、结构化展示和自动解读，从严控制信用报告打印、下载，从查询、使用和存储环节降低征信信息泄露风险。

五、建立征信信息安全事件应急处置机制

运行机构、接入机构和人民银行分支机构应逐级建立征信信息安全事件应急处置机制，成立由业务、技术、法律、宣传等方面专业人员组成的应急处置工作小组，制定应急处置方案，并自本通知发布之日起 30 个工作日内将应急处置方案向人民银行报备。报备流程参照征信内控制度及问责制度的报备要求。

六、建立征信合规与信息安全年度考核评级制度

人民银行建立接入机构征信合规与信息安全年度考核评级制度(见附件 3)。对接入机构的考核评级结果，将作为实施征信现场执法检查、中央银行对金融机构内部评级、对征信查询服务费用实行优惠、调整对征信系统的查询权限、确定金融机构存款保险评级结果和核定金融机构存款保险费率等的重要依据。

七、建立征信信息安全巡查制度

人民银行围绕上述政策措施的贯彻落实情况，针对运行机构和接入机构建立健全征信信息安全巡查制度，将巡查结论作为启动执法检查程序等的重要依据。同时，建立征信信息安全巡查内部通报制度(见附件 4)。

八、从严强化征信监管，确保征信信息安全

人民银行采取综合措施，统筹推进对运行机构和接入机构的征信监管，防范征信信息泄露风险，确保征信信息安全。

(一)强化非现场监管。

运行机构和接入机构报备的上述征信内控制度及问责制度、征信合规与信息安全自查自纠制度、征信信息安全事件应急处置方案，报告的征信信息安全事件、征信合规与信息安全自查自纠情况以及考核评级与巡查结论，均作为人民银行非现场监管的内容。对非现场监管涉及内容的真实性，人民银行将通过现场执法检查予以确认。对存在未报、漏报、虚报、瞒报情况的机构，将重点开展现场执法检查。

(二)加大现场执法检查力度。

人民银行随机对接入机构全员征信合规教育轮训情况、征信内控问责情况以及征信法规制度遵守情况进行现场执法检查，并将存在问题的机构纳入重点监管对象。对涉嫌违法违规行为的机构和人员，视情况采取监管约谈、责令限期整改、现场执法检查、在金融系统内部予以通报、向干部管理部门和纪检监察部门通报等措施，并依法从严实施行政处罚，全方位正风肃纪，促使其依法依规履职。

(三)加大违法违规成本。

对接入机构的考核评级结果、巡查结论和现场执法检查结论，将作为确定金融机构存款保险评级结果、核定金融机构存款保险费率和征信服务收费优惠与否等的重要依据；对于问题严重的机构，人民银行责成其调整其用户管理权限，直至暂停为其提供征信查询服务。

其他征信机构、信用评级机构及其接入机构的征信信息安全管理，参照本通知执行。

请人民银行副省级城市中心支行以上分支机构将本通知转发至辖区内接入机构、其他征信机构和信用评级机构。

中国银行保险监督管理委员会关于印发银行业金融机构数据治理指引的通知

基本信息：

【发布机关】中国银行保险监督管理委员会

【发文字号】银保监发〔2018〕22号

【发布日期】2018.05.21

【时效性】现行有效

【效力级别】部门规范性文件

【实施日期】2018.05.21

中国银行保险监督管理委员会关于印发银行业金融机构数据治理指引的通知

（银保监发〔2018〕22号）

各银监局，机关各部门，各政策性银行、大型银行、股份制银行，邮储银行，外资银行，金融资产管理公司，其他会管金融机构：

现将《银行业金融机构数据治理指引》印发给你们，请遵照执行。

2018年 5月 21日

银行业金融机构数据治理指引

第一章 总则

第一条 为指导银行业金融机构加强数据治理，提高数据质量，发挥数据价值，提升经营管理能力，根据《中华人民共和国银行业监督管理法》等法律法规，制定本指引。

第二条 本指引适用于中华人民共和国境内经银行业监督管理机构批准设立的银行业金融机构。

本指引所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、农村信用合作社等吸收公众存款的金融机构、政策性银行以及国家开发银行。

第三条 数据治理是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。

第四条 银行业金融机构应当将数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系。

第五条 银行业金融机构数据治理应当遵循以下基本原则：

（一）全覆盖原则。数据治理应当覆盖数据的全生命周期，覆盖业务经营、风险管理和内部控制流程中的全部数据，覆盖内部数据和外部数据，覆盖监管数据，覆盖所有分支机构和附属机构。

（二）匹配性原则。数据治理应当与管理模式、业务规模、风险状况等相适应，并根据情况变化进行调整。

（三）持续性原则。数据治理应当持续开展，建立长效机制。

（四）有效性原则。数据治理应当推动数据真实准确客观反映银行业金融机构实际情况，并有效应用于经营管理。

第六条 银行业金融机构应当将监管数据纳入数据治理，建立工作机制和流程，确保监管数据报送工作有效组织开展，监管数据质量持续提升。

法定代表人或主要负责人对监管数据质量承担最终责任。

第七条 银行业监督管理机构依据本指引对银行业金融机构数据治理情况实施监管。

第二章　数据治理架构

第八条 银行业金融机构应当建立组织架构健全、职责边界清晰的数据治理架构，明确董事会、监事会、高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。

第九条 银行业金融机构董事会应当制定数据战略，审批或授权审批与数据治理相关的重大事项，督促高级管理层提升数据治理有效性，对数据治理承担最终责任。

第十条 银行业金融机构监事会负责对董事会和高级管理层在数据治理方面的履职尽责情况进行监督评价。

第十一条 银行业金融机构高级管理层负责建立数据治理体系，确保数据治理资源配置，制定和实施问责和激励机制，建立数据质量控制机制，组织评估数据治理的有效性和执行情况，并定期向董事会报告。

银行业金融机构可根据实际情况设立首席数据官。首席数据官是否纳入高级管理人员由银行业金融机构根据经营状况确定；纳入高级管理人员管理的，应当符合相关行政许可事项的要求。

第十二条 银行业金融机构应当确定并授权归口管理部门牵头负责实施数据治理体系建设，协调落实数据管理运行机制，组织推动数据在经营管理流程中发挥作用，负责监管数据相关工作，设置监管数据相关工作专职岗位。

第十三条 业务部门应当负责本业务领域的数据治理，管理业务条线数据源，确保准确记录和及时维护，落实数据质量控制机制，执行监管数据相关工作要求，加强数据应用，实现数据价值。

第十四条 银行业金融机构应当在数据治理归口管理部门设立满足工作需要的专职岗位，在其他相关业务部门设置专职或兼职岗位。

第十五条 银行业金融机构应当建立一支满足数据治理工作需要的专业队伍，至少按年度对人员进行系统培训，科学规划职业成长通道，确定合理薪酬水平。

第十六条 银行业金融机构应当建立良好的数据文化，树立数据是重要资产和数据应真实客观的理念与准则，强化用数意识，遵循依规用数、科学用数的职业操守。

第三章　数据管理

第十七条 银行业金融机构应当结合自身发展战略、监管要求等，制定数据战略并确保有效执行和修订。

第十八条 银行业金融机构应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。

银行业金融机构应当根据监管要求和实际需要，持续评价更新数据管理制度。

第十九条 银行业金融机构应当制定与监管数据相关的监管统计管理制度和业务制度，及时发布并定期评价和更新，报银行业监督管理机构备案。制度出现重大变化的，应当及时向银行业监督管理机构报告。

第二十条 银行业金融机构应当建立覆盖全部数据的标准化规划，遵循统一的业务规范和技术标准。数据标准应当符合国家标准化政策及监管规定，并确保被有效执行。

第二十一条 银行业金融机构应当持续完善信息系统，覆盖各项业务和管理数据。信息系统应当有完备的数据字典和维护流程，并具有可拓展性。

第二十二条 银行业金融机构应当建立适应监管数据报送工作需要的信息系统，实现流程控制的程序化，提高监管数据加工的自动化程度。

第二十三条 银行业金融机构应当加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享。

第二十四条 银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

第二十五条 银行业金融机构应当加强数据资料统一管理，建立全面严密的管理流程、归档制度，明确存档交接、口径梳理等要求，保证数据可比性。

第二十六条 银行业金融机构应当建立数据应急预案，根据业务影响分析，组织开展应急演练，完善处置流程，保证在系统服务异常以及危机等情景下数据的完整、准确和连续。

第二十七条 银行业金融机构应当建立数据治理自我评估机制，明确评估周期、流程、结果应用、组织保障等要素的相关要求。

评估内容应覆盖数据治理架构、数据管理、数据安全、数据质量和数据价值实现等方面，并按年度向银行业监督管理机构报送。

第二十八条 银行业金融机构应当建立问责机制，定期排查数据管理、数据质量控制、数据价值实现等方面问题，依据有关规定对高级管理层和相关部门及责任人进行问责。

银行业金融机构应结合实际情况，建立激励机制，保障数据治理工作有效推进。

第四章　数据质量控制

第二十九条 银行业金融机构应当确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。

第三十条 银行业金融机构各项业务制度应当充分考虑数据质量管理需要，涉及指标含义清晰明确，取数规则统一，并根据业务变化及时更新。

第三十一条 银行业金融机构应当加强数据源头管理，确保将业务信息全面准确及时录入信息系统。信息系统应当能自动提示异常变动及错误情况。

第三十二条 银行业金融机构应当建立数据质量监控体系，覆盖数据全生命周期，对数据质量持续监测、分析、反馈和纠正。

第三十三条 银行业金融机构应当建立数据质量现场检查制度，定期组织实施，原则上不低于每年一次，对重大问题要按照既定的报告路径提交，并按流程实施整改。

第三十四条 银行业金融机构应当建立数据质量考核评价体系，考核结果纳入本机构绩效考核体系，实现数据质量持续提升。

第三十五条 银行业金融机构应当建立数据质量整改机制，对日常监控、检查和考核评价过程中发现的问题，及时组织整改，并对整改情况跟踪评价，确保整改落实到位。

第三十六条 银行业金融机构应当按照监管要求报送法人和集团的相关数据，保证同一监管指标在监管报送与对外披露之间的一致性。如有重大差异，应当及时向银行业监督管理机构解释说明。

第三十七条 银行业金融机构应当建立监管数据质量管控制度，包括但不限于：关键监管指标数据质量承诺、数据异常变动分析和报告、重大差错通报以及问责等。

第五章　数据价值实现

第三十八条 银行业金融机构应当在风险管理、业务经营与内部控制中加强数据应用，实现数据驱动，提高管理精细化程度，发挥数据价值。

第三十九条 银行业金融机构应当充分运用数据分析，合理制定风险管理策略、风险偏好、风险限额以及风险管理政策和程序，监控执行情况并适时优化调整，提升风险管理体系的有效性。

全球系统重要性银行应遵循更高的标准，对照有效风险数据加总与风险报告评估要点的相关要求，强化风险管理。

第四十条 银行业金融机构应当加强数据应用，持续改善风险管理方法，有效识别、计量、评估、监测、报告和控制各类风险。

第四十一条 银行业金融机构应当提高数据加总能力，明确数据加总范围、方法、流程和加总结果要求等，满足在正常经营、压力情景以及危机状况下风险管理的数据需要。

加总内容包括但不限于交易对手、产品、地域、行业、客户以及其他相关的分类。加总技术应当主要采取自动化方式。

第四十二条 银行业金融机构应当加强数据分析应用能力，提高风险报告质量，明确风险报告数据准确性保障措施，覆盖重要风险领域和新风险，提供风险处置的决策与建议以及未来风险发展趋势。

第四十三条 银行业金融机构应当加强数据积累，优化风险计量，持续完善风险定价模型，优化风险定价体系。

第四十四条 银行业金融机构应当充分评估兼并收购、资产剥离等业务对自身数据治理能力的影响。有重大影响的，应当明确整改计划和时间表，满足银行集团风险管理要求。

第四十五条 银行业金融机构应当明确新产品新服务的数据管理相关要求，确保清晰评估成本、风险和收益，并作为准入标准。

第四十六条 银行业金融机构应当通过数据分析挖掘，准确理解客户需求，提供精准产品服务，提升客户服务质量和服务水平。

第四十七条 银行业金融机构应当通过量化分析业务流程，减少管理冗余，提高经营效率，降低经营成本。

第四十八条 银行业金融机构应当充分运用大数据技术，实现业务创新、产品创新和服务创新。

第四十九条 银行业金融机构应当按照可量化导向，完善内部控制评价制度和内部控制评价质量控制机制，前瞻性识别内部控制流程的缺陷，评估影响程度并及时处理，持续提升内部控制的有效性。

第六章　监督管理

第五十条 银行业监督管理机构应当通过非现场监管和现场检查对银行业金融机构数据治理情况进行持续监管。

第五十一条 银行业监督管理机构可根据需要，要求银行业金融机构通过内部审计机构或委托外部审计机构对其数据治理情况进行审计，并及时报送审计报告。

第五十二条 对数据治理不满足《中华人民共和国银行业监督管理法》等法律法规及国务院银行业监督管理机构审慎经营规则要求的银行业金融机构，银行业监督管理机构可采取相应措施：

（一）要求其制定整改方案，责令限期改正；

（二）与公司治理评价结果或监管评级挂钩；

（三）依法采取监管措施及实施行政处罚。

第七章　附则

第五十三条 外国银行分行以及银行业监督管理机构负责监管的其他金融机构参照执行本指引。

第五十四条 本指引由国务院银行业监督管理机构负责解释。

第五十五条 本指引自印发之日起施行。《银行监管统计数据质量管理良好标准（试行）》（银监发〔2011〕63号）同时废止。

银行业金融机构数据治理指引

基本信息：

【发布机关】中国银行保险监督管理委员会

【发文字号】银保监发〔2018〕22号

【发布日期】2018.5.21

【时效性】现行有效

【效力级别】规范性文件

【实施日期】2018.5.21

银行业金融机构数据治理指引

第一章 总则

第一条 为指导银行业金融机构加强数据治理，提高数据质量，发挥数据价值，提升经营管理能力，根据《中华人民共和国银行业监督管理法》等法律法规，制定本指引。

第二条 本指引适用于中华人民共和国境内经银行业监督管理机构批准设立的银行业金融机构。

本指引所称银行业金融机构，是指在中华人民共和国境内设立的商业银行、农村信用合作社等吸收公众存款的金融机构、政策性银行以及国家开发银行。

第三条 数据治理是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。

第四条 银行业金融机构应当将数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系。

第五条 银行业金融机构数据治理应当遵循以下基本原则：

（一）全覆盖原则。数据治理应当覆盖数据的全生命周期，覆盖业务经营、风险管理和内部控制流程中的全部数据，覆盖内部数据和外部数据，覆盖监管数据，覆盖所有分支机构和附属机构。

（二）匹配性原则。数据治理应当与管理模式、业务规模、风险状况等相适应，并根据情况变化进行调整。

（三）持续性原则。数据治理应当持续开展，建立长效机制。

（四）有效性原则。数据治理应当推动数据真实准确客观反映银行业金融机构实际情况，并有效应用于经营管理。

第六条 银行业金融机构应当将监管数据纳入数据治理，建立工作机制和流程，确保监管数据报送工作有效组织开展，监管数据质量持续提升。

法定代表人或主要负责人对监管数据质量承担最终责任。

第七条 银行业监督管理机构依据本指引对银行业金融机构数据治理情况实施监管。

第二章 数据治理架构

第八条 银行业金融机构应当建立组织架构健全、职责边界清晰的数据治理架构，明确董事会、监事会、高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。

第九条 银行业金融机构董事会应当制定数据战略，审批或授权审批与数据治理相关的重大事项，督促高级管理层提升数据治理有效性，对数据治理承担最终责任。

第十条 银行业金融机构监事会负责对董事会和高级管理层在数据治理方面的履职尽责情况进行监督评价。

第十一条 银行业金融机构高级管理层负责建立数据治理体系，确保数据治理资源配置，制定和实施问责和激励机制，建立数据质量控制机制，组织评估数据治理的有效性和执行情况，并定期向董事会报告。

银行业金融机构可根据实际情况设立首席数据官。首席数据官是否纳入高级管理人员由银行业金融机构根据经营状况确定；纳入高级管理人员管理的，应当符合相关行政许可事项的要求。

第十二条 银行业金融机构应当确定并授权归口管理部门牵头负责实施数据治理体系建设，协调落实数据管理运行机制，组织推动数据在经营管理流程中发挥作用，负责监管数据相关工作，设置监管数据相关工作专职岗位。

第十三条 业务部门应当负责本业务领域的数据治理，管理业务条线数据源，确保准确记录和及时维护，落实数据质量控制机制，执行监管数据相关工作要求，加强数据应用，实现数据价值。

第十四条 银行业金融机构应当在数据治理归口管理部门设立满足工作需要的专职岗位，在其他相关业务部门设置专职或兼职岗位。

第十五条 银行业金融机构应当建立一支满足数据治理工作需要的专业队伍，至少按年度对人员进行系统培训，科学规划职业成长通道，确定合理薪酬水平。

第十六条 银行业金融机构应当建立良好的数据文化，树立数据是重要资产和数据应真实客观的理念与准则，强化用数意识，遵循依规用数、科学用数的职业操守。

第三章 数据管理

第十七条 银行业金融机构应当结合自身发展战略、监管要求等，制定数据战略并确保有效执行和修订。

第十八条 银行业金融机构应当制定全面科学有效的数据管理制度，包括但不限于组织管理、部门职责、协调机制、安全管控、系统保障、监督检查和数据质量控制等方面。

银行业金融机构应当根据监管要求和实际需要，持续评价更新数据管理制度。

第十九条 银行业金融机构应当制定与监管数据相关的监管统计管理制度和业务制度，及时发布并定期评价和更新，报银行业监督管理机构备案。制度出现重大变化的，应当及时向银行业监督管理机构报告。

第二十条 银行业金融机构应当建立覆盖全部数据的标准化规划，遵循统一的业务规范和技术标准。数据标准应当符合国家标准化政策及监管规定，并确保被有效执行。

第二十一条 银行业金融机构应当持续完善信息系统，覆盖各项业务和管理数据。信息系统应当有完备的数据字典和维护流程，并具有可拓展性。

第二十二条 银行业金融机构应当建立适应监管数据报送工作需要的信息系统，实现流程控制的程序化，提高监管数据加工的自动化程度。

第二十三条 银行业金融机构应当加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享。

第二十四条 银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问和拷贝等权限，监控访问和拷贝等行为，完善数据安全技术，定期审计数据安全。

银行业金融机构采集、应用数据涉及到个人信息的，应遵循国家个人信息保护法律法规要求，符合与个人信息安全相关的国家标准。

第二十五条 银行业金融机构应当加强数据资料统一管理，建立全面严密的管理流程、归档制度，明确存档交接、口径梳理等要求，保证数据可比性。

第二十六条 银行业金融机构应当建立数据应急预案，根据业务影响分析，组织开展应急演练，完善处置流程，保证在系统服务异常以及危机等情景下数据的完整、准确和连续。

第二十七条 银行业金融机构应当建立数据治理自我评估机制，明确评估周期、流程、结果应用、组织保障等要素的相关要求。

评估内容应覆盖数据治理架构、数据管理、数据安全、数据质量和数据价值实现等方面，并按年度向银行业监督管理机构报送。

第二十八条 银行业金融机构应当建立问责机制，定期排查数据管理、数据质量控制、数据价值实现等方面问题，依据有关规定对高级管理层和相关部门及责任人进行问责。

银行业金融机构应结合实际情况，建立激励机制，保障数据治理工作有效推进。

第四章 数据质量控制

第二十九条 银行业金融机构应当确立数据质量管理目标，建立控制机制，确保数据的真实性、准确性、连续性、完整性和及时性。

第三十条 银行业金融机构各项业务制度应当充分考虑数据质量管理需要，涉及指标含义清晰明确，取数规则统一，并根据业务变化及时更新。

第三十一条 银行业金融机构应当加强数据源头管理，确保将业务信息全面准确及时录入信息系统。信息系统应当能自动提示异常变动及错误情况。

第三十二条 银行业金融机构应当建立数据质量监控体系，覆盖数据全生命周期，对数据质量持续监测、分析、反馈和纠正。

第三十三条 银行业金融机构应当建立数据质量现场检查制度，定期组织实施，原则上不低于每年一次，对重大问题要按照既定的报告路径提交，并按流程实施整改。

第三十四条 银行业金融机构应当建立数据质量考核评价体系，考核结果纳入本机构绩

效考核体系，实现数据质量持续提升。

第三十五条 银行业金融机构应当建立数据质量整改机制，对日常监控、检查和考核评价过程中发现的问题，及时组织整改，并对整改情况跟踪评价，确保整改落实到位。

第三十六条 银行业金融机构应当按照监管要求报送法人和集团的相关数据，保证同一监管指标在监管报送与对外披露之间的一致性。如有重大差异，应当及时向银行业监督管理机构解释说明。

第三十七条 银行业金融机构应当建立监管数据质量管控制度，包括但不限于：关键监管指标数据质量承诺、数据异常变动分析和报告、重大差错通报以及问责等。

第五章 数据价值实现

第三十八条 银行业金融机构应当在风险管理、业务经营与内部控制中加强数据应用，实现数据驱动，提高管理精细化程度，发挥数据价值。

第三十九条 银行业金融机构应当充分运用数据分析，合理制定风险管理策略、风险偏好、风险限额以及风险管理政策和程序，监控执行情况并适时优化调整，提升风险管理体系的有效性。

全球系统重要性银行应遵循更高的标准，对照有效风险数据加总与风险报告评估要点的相关要求，强化风险管理。

第四十条 银行业金融机构应当加强数据应用，持续改善风险管理方法，有效识别、计量、评估、监测、报告和控制各类风险。

第四十一条 银行业金融机构应当提高数据加总能力，明确数据加总范围、方法、流程和加总结果要求等，满足在正常经营、压力情景以及危机状况下风险管理的数据需要。

加总内容包括但不限于交易对手、产品、地域、行业、客户以及其他相关的分类。加总技术应当主要采取自动化方式。

第四十二条 银行业金融机构应当加强数据分析应用能力，提高风险报告质量，明确风险报告数据准确性保障措施，覆盖重要风险领域和新风险，提供风险处置的决策与建议以及未来风险发展趋势。

第四十三条 银行业金融机构应当加强数据积累，优化风险计量，持续完善风险定价模型，优化风险定价体系。

第四十四条 银行业金融机构应当充分评估兼并收购、资产剥离等业务对自身数据治理能力的影响。有重大影响的，应当明确整改计划和时间表，满足银行集团风险管理要求。

第四十五条 银行业金融机构应当明确新产品新服务的数据管理相关要求，确保清晰评

估成本、风险和收益，并作为准入标准。

第四十六条 银行业金融机构应当通过数据分析挖掘，准确理解客户需求，提供精准产品服务，提升客户服务质量和服务水平。

第四十七条 银行业金融机构应当通过量化分析业务流程，减少管理冗余，提高经营效率，降低经营成本。

第四十八条 银行业金融机构应当充分运用大数据技术，实现业务创新、产品创新和服务创新。

第四十九条 银行业金融机构应当按照可量化导向，完善内部控制评价制度和内部控制评价质量控制机制，前瞻性识别内部控制流程的缺陷，评估影响程度并及时处理，持续提升内部控制的有效性。

第六章 监督管理

第五十条 银行业监督管理机构应当通过非现场监管和现场检查对银行业金融机构数据治理情况进行持续监管。

第五十一条 银行业监督管理机构可根据需要，要求银行业金融机构通过内部审计机构或委托外部审计机构对其数据治理情况进行审计，并及时报送审计报告。

第五十二条 对数据治理不满足《中华人民共和国银行业监督管理法》等法律法规及国务院银行业监督管理机构审慎经营规则要求的银行业金融机构，银行业监督管理机构可采取相应措施：

（一）要求其制定整改方案，责令限期改正；

（二）与公司治理评价结果或监管评级挂钩；

（三）依法采取监管措施及实施行政处罚。

第七章 附则

第五十三条 外国银行分行以及银行业监督管理机构负责监管的其他金融机构参照执行本指引。

第五十四条 本指引由国务院银行业监督管理机构负责解释。

第五十五条 本指引自印发之日起施行。《银行监管统计数据质量管理良好标准（试行）》（银监发〔2011〕63号）同时废止。

网络小额贷款从业机构反洗钱和反恐怖融资工作指引

基本信息：

【发布机关】中国互联网金融协会	【时效性】现行有效
【发文字号】银发〔2018〕230号	【效力级别】规范性文件
【发布日期】2018.10.10	【实施日期】2018.10.10

网络小额贷款从业机构反洗钱和反恐怖融资工作指引

第一章 总则

第一条 为防范洗钱和恐怖融资活动，规范网络小额贷款机构反洗钱和反恐怖融资工作，根据《中华人民共和国反洗钱法》《中华人民共和国反恐怖主义法》《金融机构反洗钱规定》《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》等有关规定，制定本指引。

第二条 本指引适用于在中华人民共和国境内经有权部门批准设立的依法可通过互联网专门经营小额贷款业务的机构（以下统称“从业机构”）。

第三条 从业机构开展反洗钱和反恐怖融资（以下统称“反洗钱”）工作应当遵循风险为本原则，开展洗钱和恐怖融资风险（以下统称“洗钱风险”）评估，完善反洗钱风险管理机制，加强反洗钱合规管理和反洗钱工具创新，有效防控洗钱风险。

从业人员应当勤勉尽责，主动履行反洗钱义务。

第四条 从业机构应当依法接受中国人民银行及其分支机构的反洗钱现场检查、非现场监管和反洗钱调查，不得拒绝、阻挠、逃避检查、监管和反洗钱调查，不得谎报、隐匿、销毁相关信息、数据和资料。

从业机构应当依法接受国务院有关金融监督管理机构及其派出机构、地方金融监管机构的监督管理。

第五条 中国互联网金融协会按照中国人民银行、国务院有关金融监督管理机构关于从业机构履行反洗钱义务的规定，协调其他行业自律组织，制定并发布从业机构所适用的反洗钱行业规则；配合中国人民银行及其分支机构开展线上和线下反洗钱相关工作，开展洗钱风险评估，发布风险评估报告和风险提示信息；组织推动各类从业机构制定并实施反洗钱方面的自律公约。

其他行业自律组织按照中国人民银行、中国银行保险监督管理委员会等监管机构的规定对从业机构提出建立健全反洗钱内控制度的要求，配合中国互联网金融协会推动从业机构之间的业务交流和信息共享。

从业机构应当依法或按照相关自律公约接受中国互联网金融协会和其他行业自律组织对其反洗钱工作的自律管理。

第六条 从业机构应当保守反洗钱工作秘密，遵守数据合规要求。

从业机构及从业人员对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息及对报告可疑交易、配合中国人民银行及其分支机构开展反洗钱调查等有关反洗钱工作信息应当予以保密。非依法律规定，不得向任何单位和个人提供。

第七条 从业机构应当建立健全反洗钱风险管理体系、内控机制，制定和完善各项制度和操作规程，明确董事会、监事会、高级管理层、各部门和从业人员的反洗钱职责，合理配置反洗钱风险管理及合规管理资源，确保反洗钱措施的合规性和有效性。

从业机构应当建立统一的反洗钱合规管理政策，对其境内外附属机构、分支机构、事业部的反洗钱工作实施统一管理。

第八条 从业机构应当定期，或根据监管政策或自律管理要求，在业务模式、交易方式发生重大变化、拓展新的业务领域、洗钱风险状况发生较大变化时，适时评估、审核反洗钱措施和洗钱风险评估方法的有效性，并及时予以完善。

第九条 从业机构应当以单一客户为单位，实施客户反洗钱风险管理并开展客户身份识别、可疑交易监测等相关工作。

第二章 客户身份识别

第十条 从业机构应当勤勉尽责，建立健全客户身份识别制度，遵循“了解你的客户”原则，针对具有不同洗钱风险特征的客户、业务关系或者交易采取相应的合理措施，了解非自然人客户的受益所有人情况，了解自然人客户的交易是否为本人操作和交易的实际受益人。

经办人为有权代表客户办理业务的工作人员或代理人的，从业机构应当确认授权存在及授权内容、授权范围的真实性、有效性，识别和验证代理人身份。

客户及其受益所有人、经办人属于外国政要、国际组织的高级管理人员及其特定关系人的，从业机构应当采取更为严格的客户身份识别措施。

第十一条 从业机构不得为身份不明或者拒绝身份查验的客户提供服务或者与其进行交易，不得为客户开立匿名账户或者假名账户，不得与明显具有非法目的的客户建立业务关系。

从业机构应当在建立业务关系之前，完成客户及其受益所有人的身份核实工作，但为不影响正常交易，可以在有效管理洗钱风险的情况下先行建立业务关系，再尽快完成身份核实。在未完成客户身份核实工作前，从业机构应当采取必要的风险管理措施，包括但不

限于加强交易监测，限制交易数量、类型或金额等。

第十二条 在以下情形下，从业机构应当识别和核验客户或经办人的身份，了解受益所有人情况，了解建立业务关系或办理业务的目的和意图：

（一）客户建立授信业务关系或其他金融业务关系；

（二）对客户的真实身份产生怀疑的；

（三）先前已经获取的客户身份信息的真实性或有效性存疑的。

从业机构在与客户建立授信业务关系或其他金融业务关系时，应当登记客户的身份基本信息、受益所有人信息及其他相关信息，留存客户有效身份证件或证明文件的复印件、影印件或其数字文件、影像信息。

第十三条 从业机构识别和核验客户身份时，应当获得并查验足以证明客户或经办人真实身份的身份证件、身份证明文件的原件或其数字文件、影像信息，通过比对辅助身份证明文件、查验国家机关和行业自律组织数据或者其他可靠的、独立来源信息等方式，验证客户或经办人提供的身份证件、身份证明文件的原件或其数字文件、影像信息的真实性、有效性，确认身份证件、身份证明文件所记载的信息、自然人生物特征等与客户或经办人相符。

第十四条 对于累计交易额超过 1万人民币或等值美元的客户或出现疑似洗钱等高风险特征的客户，从业机构应当采取以下一种或多种措施，核验客户身份信息：

（一）实地尽职调查；

（二）比对辅助身份证明文件；

（三）查询国家机关相关数据库；

（四）查询社会组织相关数据库；

（五）通过其他从业机构或金融机构鉴权；

（六）核对金融交易凭证或其他可信交易凭证；

（七）通过金融市场、金融基础设施验证；

（八）通过信息通讯、交通、公用设施等进行验证；

（九）通过第三方中介组织尽职调查验证；

（十）对非自然人客户的法定代表人、高级管理层、控股股东等自然人进行身份核验；

（十一）依法验证生物性信息；

（十二）通过其他可靠的独立来源或渠道验证。

第十五条 从业机构按照本指引第十四条所列渠道核验自然人客户身份信息的，应符合以下要求：

（一）对自然人客户给予大于 1 万元人民币或等值美元但不超过 10 万元人民币或等值美元的一次性授信或者大于 5 万元人民币或等值美元但不超过 15 万元人民币或等值美元的综合授信时，应当至少采取两种方式核实客户身份；

（二）对自然人客户给予大于 10 万元人民币或等值美元但不超过 20 万元人民币或等值美元的一次性授信，或者大于 15 万元人民币或等值美元但不超过 30 万元人民币或等值美元的综合授信时，应当至少采取三种方式核实客户身份；

（三）对自然人客户给予超过 20 万元人民币或等值美元的一次性授信，或者超过 30 万元人民币或等值美元的综合授信时，应当至少采取四种方式核实客户身份。

对于再次给予客户授信的，从业机构可根据实际风险状况，信赖上一次的有效身份核验结果，同时确保身份核验渠道满足本条前款规定。

第十六条 从业机构按照本指引第十四条核验非自然人客户身份信息时，应符合以下要求：

（一）对非自然人客户给予大于 10 万元人民币或等值美元但不超过 50 万元人民币或等值美元的一次性授信或者大于 20 万元人民币或等值美元但不超过 100 万元人民币或等值美元的综合授信时，应当至少采取两种方式核实客户身份；

（二）对非自然人客户给予大于 50 万元人民币或等值美元但不超过 100 万元人民币或等值美元的一次性授信，或者大于 100 万元人民币或等值美元但不超过 200 万元人民币或等值美元的综合授信时，应当至少采取三种方式核实客户身份；

（三）对非自然人客户给予超过 100 万元人民币或等值美元的一次性授信，或者超过 200 万元人民币或等值美元的综合授信时，应当至少采取四种方式核实客户身份。

对非自然人客户的法定代表人、经办人等进行身份核验，且满足第十四条所列自然人身份核验方式的，可以作为非自然人客户身份核验的方式之一。

第十七条 与非自然人客户建立业务关系以及业务关系存续期间按照规定应当开展客户身份识别的，从业机构应当按照中国人民银行规定的标准和程序，识别客户的受益所有人，登记受益所有人姓名、地址、身份证或者身份证证明文件的种类、号码和有效期限。

第十八条 从业机构应当识别客户或其受益所有人是否为国外政要、国际组织高级管理人员及其关系密切人。

从业机构与国外政要及其关系密切人建立业务前应经过高级管理层批准，并将其纳入高风险客户进行管理，并对其采取强化的客户身份识别措施。

从业机构与国际组织高级管理人员及其关系密切人的业务关系出现高风险时，从业机构也应采取上述措施。

第十九条 在与客户的业务关系存续期间，从业机构应当采取持续的客户身份识别措施，审核客户身份资料和交易记录，及时更新客户身份识别相关的证明文件、数据和信息，确保客户正在进行的交易与从业机构所掌握的客户资料、客户业务、风险状况等匹配。对于高风险客户，从业机构应当采取合理措施了解其资金来源，提高审核频率。对于低风险客户，从业机构可以采取简化的措施。

第二十条 从业机构应该至少在身份证件或身份证明文件有效期满日三十天前，通知客户或经办人及时更新身份证件或身份证明文件。客户或经办人如果不能在有效期满日后的三个月内提交有效身份证件或身份证明文件且无合理理由的，从业机构不能为客户提供新的金融服务。

从业机构应当定期了解非自然人客户的运营状态和身份信息的有效性，至少每半年审核一次高风险非自然人客户，至少每三年审核一次低风险非自然人客户。

第二十一条 发生以下情形时，从业机构应当重新识别和核验客户身份，留存发生变化的身份信息资料：

（一）客户要求变更姓名或者名称、有效身份证件种类、身份证件号码、注册资本、经营范围、法定代表人或者负责人等的；

（二）对先前获得的客户身份资料存疑的；

（三）发现或怀疑涉及匿名交易、假名交易、出借账户、盗用身份证件等异常情形而需要验明客户身份的；

（四）从业机构认为应重新识别客户身份的其他情形。

第二十二条 从业机构应当建立客户洗钱风险评估标准，根据客户性质、地域、职业或所在行业、涉及的金融产品或服务以及客户是否为外国政要等因素，确定客户的洗钱风险等级。

第二十三条 从业机构应当在与客户建立业务关系十个工作日内，确定客户的洗钱风险等级，并在业务关系存续期间，定期或根据监管及自律管理要求、突发情况、重要风险事件等实际需要，评估客户风险和调整客户风险等级。

从业机构至少每半年评估一次风险等级最高客户的风险，至少每三年评估一次风险等级最低客户的风险。

第二十四条 对同一客户联合授信的从业机构，应当各自承担客户身份识别及其他反洗钱责任，并按照联合授信总额执行本指引第十五条、第十六条的要求。

联合授信的从业机构之间可以约定，由其中一家独立或几家联合具体实施客户身份识别措施，并确保任何一方在办理业务时能及时获得其他方提供的客户身份基本信息，和在必要时从其他方获得客户的有效身份证件、证明文件的复印件、影印件或其数字文件、影像信息等其他信息或资料。

第二十五条 从业机构委托其他从业机构、金融机构向客户销售金融产品、引荐客户时，应在委托协议中明确双方在识别客户身份和其他反洗钱工作方面的职责，相互间提供必要的协助，相应采取有效的客户身份识别等反洗钱措施。

符合下列条件的，从业机构可信赖金融产品销售方或客户引荐方所提供的客户身份识别结果，不再重复进行已完成的客户身份识别程序，但仍应承担未履行客户身份识别义务的责任：

（一）金融产品销售方或客户引荐方受到了严格的反洗钱监管；

（二）金融产品销售方或客户引荐方采取的客户身份识别措施符合反洗钱法律、行政法规、反洗钱监管规定和本指引的要求；

（三）从业机构能够有效获得并保存客户身份资料信息；

（四）双方数据信息交互及数据合规工作符合反洗钱自律公约等行业规则要求。

从业机构通过中国人民银行、国务院有关金融监管机构及其授权机构或依法承担反洗钱自律管理职责的自律组织建立的金融基础设施或市场交易机制获取客户身份识别结果的，可以不再进行信息核验。

第二十六条 从业机构委托其他机构代为履行客户身份识别义务时，应通过书面协议明确双方在客户身份识别方面的责任，并符合以下要求：

（一）能够证明受托方按反洗钱法律、行政法规、反洗钱监管规定和本指引的要求，采取客户身份识别和身份资料保存的必要措施；

（二）受托方为本机构提供客户信息，不存在法律制度、技术等方面的障碍；

（三）本机构在办理业务时，能及时获得受托方提供的客户身份基本信息，并在必要时从受托方获得客户的有效身份证件、证明文件影印件等其他信息或资料；

（四）双方数据信息交互及数据合规工作应符合反洗钱自律公约等行业规则要求。

受托方未采取符合本指引要求的客户身份识别措施的，由从业机构承担未履行客户身份识别义务的法律责任。

第三章 大额交易和可疑交易报告

第二十七条 从业机构应对全部客户及其全部金融业务开展监测和分析，并按规定报告

大额交易和可疑交易。

从业机构监测分析交易的维度应至少包括单一客户为单位。

第二十八条 客户当日单笔或者累计交易人民币 5 万元以上、外币等值 1 万美元以上的现金收支，从业机构应当在交易发生后的 5 个工作日内按照规定向中国反洗钱监测分析中心提交大额交易报告。

第二十九条 从业机构应当建立健全可疑交易监测机制，有效整合数据资源，加强技术研发和流程管理，并定期或根据监管和自律管理要求、突发情况、重要风险事件等实际需要，评估和完善监控机制、策略或方案。

从业机构应当制定本机构的交易监测标准，并对其有效性负责。交易监测标准包括并不限于客户的身份、行为，交易资金来源、金额、频率、流向、性质等存在异常的情形，并应当参考以下因素：

（一）中国人民银行及其分支机构发布的反洗钱规定及指引、风险提示、洗钱类型分析报告和风险评估报告。

（二）行政机关、司法机关发布的犯罪形势分析、风险提示、犯罪类型报告和工作报告。

（三）中国互联网金融协会发布的行业规则、风险提示、自律管理要求。

（四）本机构的资产规模、地域分布、业务特点、客户群体、交易特征，洗钱风险评估结论。

（五）中国人民银行及其分支机构出具的反洗钱监管意见。

（六）中国人民银行及其分支机构要求关注的其他因素。

对于规则化的交易监测指标，从业机构应在指标实际投入运行后的十个工作日内按照规定报中国反洗钱监测分析中心备案。

第三十条 从业机构发现或者有合理理由怀疑客户、客户的资金或者其他资产、客户的交易或者试图进行的交易与洗钱、恐怖融资等犯罪活动相关的，不论所涉资金金额或者资产价值大小，应当提交可疑交易报告。

从业机构应当完整保存对异常交易进行识别、分析和判断的工作记录及相关资料，包括未最终提交可疑交易报告的。

第三十一条 从业机构应当对下列恐怖活动组织及恐怖活动人员名单开展实时监测，有合理理由怀疑客户或者其交易对手、资金或者其他资产与监控名单相关的，应当按照规定立即向中国反洗钱监测分析中心提交可疑交易报告，并依法向公安机关、国家安全机关等

部门报告。客户与监控名单匹配的，应当中止与客户建立业务关系或中止提供金融服务，并在确认后 24 小时内提交可疑交易报告，并以电子形式或书面形式向所在地中国人民银行或者其分支机构报告，并按照相关主管部门的要求依法采取措施：

（一）中国政府发布的或者要求执行的恐怖活动组织及恐怖活动人员名单。

（二）联合国安理会决议中所列的恐怖活动组织及恐怖活动人员名单。

（三）中国人民银行要求关注的其他涉嫌恐怖活动的组织及人员名单。

第三十二条 从业机构应当建立健全针对恐怖活动组织、恐怖活动人员和其他应对其实施实时反洗钱监测的机构、个人的名单监控机制，并对与监控名单上的机构、人员存在重要关联关系或密切经济往来的其他客户加强监测分析。

经使用合理手段无法判断客户与监控名单是否一致，但无法排除怀疑的，从业机构应当提交可疑交易报告，并进行持续交易监测分析。

监控名单发生调整的，从业机构应当立即对现有客户和三年内发生过交易的其他客户进行回溯性调查，并按规定提交可疑交易报告。发布监控名单的有权机关对回溯性调查另有规定或要求的，遵守其规定或要求。

第三十三条 对于恐怖活动组织及恐怖活动人员归还贷款的，从业机构应当立即冻结偿贷资金，并向有权机关进行报告，按要求处理资金。

第三十四条 从业机构提交可疑交易报告后，应当对相关客户及交易进行持续监测，仍不能排除洗钱、恐怖融资或其他犯罪活动嫌疑，且经分析认为可疑特征没有发生显著变化的，应当自上一次提交可疑交易报告之日起每三个月提交一次接续报告。接续报告应当包括三个月监测期内的新增交易，并注明首次提交可疑交易报告号、报告紧急程度和追加次数。

第三十五条 从业机构应当在按本机构可疑交易报告内部操作规程确认为可疑交易后，及时以电子方式向中国反洗钱监测分析中心提交可疑交易报告。可疑交易报告的具体格式和报送方式执行中国人民银行的规定。

第三十六条 从业机构应当提供真实、完整、准确的交易信息，在接到中国反洗钱监测分析中心发出的补正通知之日起十个工作日内予以补正。

第三十七条 可疑交易符合下列情形之一的，从业机构应当在向中国反洗钱监测分析中心提交可疑交易报告的同时，以电子或书面形式向所在地中国人民银行或者其分支机构报告，并配合反洗钱调查：

（一）明显涉嫌洗钱、恐怖融资等犯罪活动的；

（二）严重危害国家安全或者影响社会稳定的；

（三）其他情节严重或者情况紧急的情形。

对已经提交可疑交易报告的客户，应根据客户不同异常情形采取相应措施，对重点可疑的客户加强控制措施。

第三十八条 从业机构应当针对可疑交易报告所涉及的客户和业务，依法采取适当的后续控制措施，包括但不限于提高监测频率及强度、限制借款方式、限制借款规模或频率、退出客户关系等。

第四章 客户身份资料和交易记录保存

第三十九条 从业机构应当妥善保存客户身份资料和交易记录，保证能够完整、准确地重现每笔交易。

第四十条 从业机构应当保存的客户身份资料包括各种记载客户身份信息的资料、辅助证明客户身份的资料和反映从业机构开展客户身份识别工作情况的资料。

从业机构应当完整保存借（还）款人名称、借（还）款金额、借（还）款时间，借（还）款所涉及的银行名称及银行账号、支付机构名称及支付账户号等记录资金来源和去向的信息等记录，确保交易全程可追溯。

第四十一条 从业机构应当建立客户身份资料和交易记录保存系统，实时记载操作记录，及时发现并追踪任何不合规操作或未经授权操作活动，防止客户身份信息和交易记录的泄露、损毁和缺失，防止客户信息和交易数据被篡改。

第四十二条 从业机构应当完善客户身份资料和交易记录保存系统的查询和分析功能，便于反洗钱调查和监督管理。

第四十三条 从业机构应当按照下列期限保存客户身份资料和交易记录：

（一）客户身份资料，自业务关系结束当年计起至少保存 5 年；

（二）交易记录，自交易记账当年计起至少保存 5 年。

如客户身份资料和交易记录涉及反洗钱调查，且反洗钱调查工作在前款规定的最低保存期届满时仍未结束的，从业机构应将其保存至反洗钱调查工作结束。

同一介质上存有不同保存期限客户身份资料或者交易记录的，应当按最长期限保存。同一客户身份资料或者交易记录采用不同介质保存的，至少应当按照上述期限要求保存一种介质的客户身份资料或者交易记录。

法律、行政法规、规章和监管制度对客户身份资料和交易记录有更长保存期限要求的，遵守其规定。

第五章 风险管理与内控机制

第四十四条 从业机构应当科学评估洗钱风险与市场风险、操作风险等其他风险的关联性，确保各项风险管理政策协调一致，积极发挥业务条线（部门）在了解客户方面的基础性作用，避免反洗钱工作职责空洞化。

第四十五条 反洗钱风险控制体系应当全面覆盖各项金融产品或金融服务。

从业机构应从全流程管理的角度对各项金融业务进行系统性的洗钱风险评估，并按照风险为本的原则，强化风险较高领域的反洗钱合规管理措施，防范从业人员的专业知识和专业技能被不法分子所利用。

从业机构在研发创新型金融产品、对存量产品使用新技术和拓展新渠道的过程中，应进行洗钱风险评估，并书面记录风险评估情况。

第四十六条 从业机构应当定期开展反洗钱内部审计，加强对业务条线（部门）或其分支机构反洗钱工作的检查，及时发现并纠正反洗钱工作中出现的不合规问题。

第四十七条 从业机构应当增强内部反洗钱工作报告路线的独立性和灵活性，完善内部管理制约机制，实施董事会、监事会对高级管理层的有效监督和高级管理层对其金融从业人员的有效监控，防范内部人员参与违法犯罪活动。

从业机构应当建立违规事件举报机制，切实保障每一位员工均有权利并通过适当的途径举报违规事件。

第四十八条 从业机构应当建立反洗钱培训长效机制，确保从业人员具备反洗钱履职所需的各项能力，并适当提高对于从事洗钱风险较高岗位的从业人员进行反洗钱培训的强度和频率。

第四十九条 从业机构应当及时梳理与本机构有关的金融违法案件信息，及时妥善处理从业人员反洗钱履职问题。

第六章 合规管理和行业自律

第五十条 从业机构应当对中国人民银行及其分支机构实施的反洗钱调查予以积极配合，如实提供调查资料，不得拒绝或阻碍调查。从业机构及其工作人员拒绝、阻碍反洗钱调查，拒绝提供调查材料或者故意提供虚假材料的，依法承担相应法律责任。

第五十一条 中国互联网金融协会按照中国人民银行和国务院有关金融监督管理机构的要求建设、运行和维护互联网金融反洗钱和反恐怖融资网络监测平台（以下简称“网络监测平台”），确保网络监测平台及相关信息、数据和资料的安全、保密、完整。

从业机构登录网络监测平台和实施操作，应当遵守网络监测平台的操作规范，并指定

专人负责，及时查看和处理中国人民银行及其分支机构、中国互联网金融协会通过网络监测平台发布的任务通知，按要求进行回复和报告。

第五十二条 中国互联网金融协会和中国小额贷款公司协会、其他行业自律组织建立健全反洗钱工作合作机制，在遵守相关法律法规、监管政策、工作纪律的前提下，依据各自章程的规定，共享涉及对方会员单位的自律管理信息和行业通用信息。

第五十三条 从业机构应当自获准经营网络小额贷款业务之日起十个工作日内通过网络监测平台向中国人民银行进行反洗钱履职登记，按要求填报信息并提交资料。已登记信息发生变更的，从业机构应当在相关事实发生后的十个工作日内进行更新相关信息。

第五十四条 从业机构应当按照中国人民银行制定的反洗钱信息报告制度及反洗钱监管档案管理办法的要求，通过网络监测平台和其他规定途径提交反洗钱报告、报表及其他信息资料。

第五十五条 从业机构应当对所报送或共享的信息资料的合法性、真实性、准确性、完整性和有效性负责，并按照中国人民银行及其分支机构、中国互联网金融协会的要求，及时补正所提交的信息资料，或对所报送信息进行说明或解释。

第五十六条 从业机构应当按照中国人民银行的规定，撰写反洗钱年度报告，在每年第一季度内通过网络监测平台报告以下内容：

（一）反洗钱工作的整体情况及机构概况；

（二）反洗钱工作机制建立情况；

（三）反洗钱法定义务履行情况；

（四）反洗钱工作配合与成效情况；

（五）其他反洗钱工作情况、问题及建议。

从业机构有境外机构的，由其境内法人机构总部按年度报告所属境外机构接受驻在国家（地区）反洗钱监管的情况。

第五十七条 从业机构发生下列情况的，应当在十个工作日内通过网络监测平台报告：

（一）反洗钱内控制度制定和修改情况；

（二）反洗钱风险管理制度的建设和调整情况；

（三）高级管理层和反洗钱负责人信息，反洗钱工作机构、岗位人员信息发生调整的；

（四）涉及本机构的反洗钱重大违规行为、洗钱案件、处罚信息；

（五）涉及本机构反洗钱工作的重大风险事项；

（六）洗钱风险自评估报告或其他相关风险评估材料；

（七）其他由中国人民银行明确要求立即报告的涉及反洗钱事项。

第五十八条 从业机构应当按照中国人民银行及其分支机构的部署安排开展反洗钱风险评估和考核评级工作，通过网络监测平台或其他规定的途径提交评估考核资料信息。中国互联网金融协会应当按照中国人民银行及其分支机构的要求，配合开展风险评估和考核评级，督促从业机构如实报告和按要求整改。

第五十九条 从业机构及其从业人员应当接受中国人民银行及其分支机构、中国互联网金融协会对其反洗钱工作情况的质询，予以及时回复、确认，不得拒绝、隐瞒或故意拖延。

第六十条 中国互联网金融协会应当按照中国人民银行、国务院有关金融监管机构的要求和自律管理工作需要，建立健全从业机构反洗钱风险评估机制，组织行业和从业机构开展洗钱风险评估工作，采取适当方式发布风险评估结果，运用风险评估结果完善反洗钱工作机制。

中国互联网金融协会应当按照洗钱风险程度，对从业机构、从业人员和互联网金融产品分类实施反洗钱自律管理。

第六十一条 从业机构及其董事、高级管理人员和相关工作人员，应当按照中国人民银行及其分支机构的要求，接受约见和警示谈话，对反洗钱工作有关事项作出说明。

第六十二条 出现以下情形时，中国互联网金融协会应采取问询、查阅复制资料、调查分析、自律检查等方式，向从业机构及从业人员了解情况，评估风险：

（一）从业机构、从业人员涉嫌存在违反反洗钱规定的行为；

（二）从业机构、从业人员涉及重大洗钱案件；

（三）行业或从业机构、从业人员涉及有关重大洗钱案件的新闻报道；

（四）中国人民银行、国务院有关金融监管机构和地方金融监管机构提出监管意见或建议；

（五）其他应当开展自律检查调查的情形。

第六十三条 中国互联网金融协会发现从业机构、从业人员违反反洗钱规定或行业存在较重大洗钱风险的，应当及时向中国人民银行、国务院有关金融监管机构和地方金融监管机构报告。

第六十四条 从业机构、从业人员和中国互联网金融协会发现洗钱案件线索的，应当立即向有管辖权的侦查机关报案。

第六十五条 从业机构及从业人员违反本指引的，中国互联网金融协会可以对其采取以

下自律管理措施，并可以向行业发出风险提示：

（一）发送风险提示函；

（二）建议整改；

（三）约见谈话；

（四）建议培训；

（五）以适当方式向社会公众进行通报；

（六）向中国人民银行、国务院有关金融监督管理机构报告；

（七）其他自律管理措施。

第六十六条 中国互联网金融协会会员单位、签署反洗钱自律公约的单位及其工作人员违反本指引的，中国互联网金融协会应当责令其立即整改，并可以按照相关自律公约采取以下自律惩戒措施：

（一）警示约谈；

（二）发警示函；

（三）强制培训；

（四）业内通报；

（五）公开谴责；

（六）自律公约规定的其他惩戒措施。

第七章 附则

第六十七条 本办法相关用语含义如下：

中国人民银行分支机构，包括中国人民银行上海总部、分行、营业管理部、省会（首府）城市中心支行、副省级城市中心支行。

金融机构是指依法设立的从事金融业务的政策性银行、商业银行、农村合作银行、农村信用社、村镇银行、证券公司、期货公司、基金管理公司、保险公司、保险资产管理公司、保险专业代理公司、保险经纪公司、信托公司、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、贷款公司以及中国人民银行确定并公布的从事金融业务的其他机构。

自然人客户的有效身份证件包括:1.在中华人民共和国境内已登记常住户口的中国公民为居民身份证；不满十六周岁的，可以使用居民身份证或户口簿。2.香港、澳门特别行政区居民为港澳居民往来内地通行证。3.台湾地区居民为台湾居民来往大陆通行证。4.定居国

外的中国公民为中国护照。5.外国公民为护照或者外国人永久居留证（外国边民，按照边贸结算的有关规定办理）。6.法律、行政法规规定的其他身份证明文件。辅助身份证明材料包括但不限于:1.中国公民为户口簿、护照、机动车驾驶证、居住证、社会保障卡、军人和武装警察身份证件、公安机关出具的户籍证明、工作证。2.香港、澳门特别行政区居民为香港、澳门特别行政区居民身份证。3.台湾地区居民为台湾居住的有效身份证明。4.定居国外的中国公民为定居国外的证明文件。5.外国公民为外国居民身份证、使领馆人员身份证件或者机动车驾驶证等其他带有照片的身份证件。6.完税证明、水电煤缴费单等税费证明。军人、武装警察尚未领取居民身份证的，除出具军人和武装警察身份证件外，还应出具军人保障卡或所在单位开具的尚未领取居民身份证的证明材料。

非自然人客户的有效身份证件或证明文件为经有权部门核发的可证明该客户依法设立或者可依法开展经营、社会活动的执照、证件或者文件。

自然人客户的“身份基本信息”包括客户的姓名、性别、国籍、职业、住所地或者工作单位地址、联系方式，身份证件或者身份证明文件的种类、号码和有效期限。客户的住所地与经常居住地不一致的，登记客户的经常居住地。

法人、其他组织和个体工商户客户的“身份基本信息”包括客户的名称、住所、经营范围；身份证件或证明文件的名称、号码和有效期限；控股股东或者实际控制人、法定代表人、负责人和授权办理业务人员的姓名、身份证件或者身份证明文件的种类、号码、有效期限。

业务如无特殊说明，仅指从业机构依法可经营的金融业务。

以上含本数。

第六十八条 本指引由中国互联网金融协会负责解释。

第六十九条 本指引自发布之日起施行。

发布前已成立但尚未进行反洗钱履职登记的从业机构应当在本指引发布之日起三十天内通过网络监测平台进行反洗钱履职登记。

互联网金融从业机构反洗钱和反恐怖融资管理办法

基本信息：

【发布机关】中国人民银行等十部门	【时效性】现行有效
【发文字号】银发〔2018〕230号	【效力级别】部门规章
【发布日期】2018.10.10	【实施日期】2019.01.01

互联网金融从业机构反洗钱和反恐怖融资管理办法

第一条　为了预防洗钱和恐怖融资活动，规范互联网金融行业反洗钱和反恐怖融资工作，根据《中华人民共和国中国人民银行法》、《中华人民共和国反洗钱法》、《中华人民共和国反恐怖主义法》、《国务院办公厅关于印发互联网金融风险专项整治工作实施方案的通知》（国办发〔2016〕21号）、《中国人民银行 工业和信息化部 公安部 财政部 工商总局 法制办 银监会 证监会 保监会 国家互联网信息办公室关于促进互联网金融健康发展的指导意见》（银发〔2015〕221号）等规定，制定本办法。

第二条　本办法适用于在中华人民共和国境内经有权部门批准或者备案设立的，依法经营互联网金融业务的机构（以下简称从业机构）。

互联网金融是利用互联网技术和信息通信技术实现资金融通、支付、投资及信息中介服务的新型金融业务模式。互联网金融业务反洗钱和反恐怖融资工作的具体范围由中国人民银行会同国务院有关金融监督管理机构按照法律规定和监管政策确定、调整并公布，包括但不限于网络支付、网络借贷、网络借贷信息中介、股权众筹融资、互联网基金销售、互联网保险、互联网信托和互联网消费金融等。

金融机构和非银行支付机构开展互联网金融业务的，应当执行本办法的规定；中国人民银行、国务院有关金融监督管理机构另有规定的，从其规定。

第三条　中国人民银行是国务院反洗钱行政主管部门，对从业机构依法履行反洗钱和反恐怖融资监督管理职责。国务院有关金融监督管理机构在职责范围内配合中国人民银行履行反洗钱和反恐怖融资监督管理职责。中国人民银行制定或者会同国务院有关金融监督管理机构制定从业机构履行反洗钱和反恐怖融资义务的规章制度。

中国人民银行设立的中国反洗钱监测分析中心，负责从业机构大额交易和可疑交易报告的接收、分析和保存，并按照规定向中国人民银行报告分析结果，履行中国人民银行规定的其他职责。

第四条　中国互联网金融协会按照中国人民银行、国务院有关金融监督管理机构关于从业机构履行反洗钱和反恐怖融资义务的规定，协调其他行业自律组织，制定并发布各类从业机构执行本办法所适用的行业规则；配合中国人民银行及其分支机构开展线上和线下反洗钱相关工作，开展洗钱和恐怖融资风险评估，发布风险评估报告和风险提示信息；组织推动各类从业机构制定并实施反洗钱和反恐怖融资方面的自律公约。

其他行业自律组织按照中国人民银行、国务院有关金融监督管理机构的规定对从业机构提出建立健全反洗钱内控制度的要求，配合中国互联网金融协会推动从业机构之间的业务交流和信息共享。

第五条　中国人民银行设立互联网金融反洗钱和反恐怖融资网络监测平台（以下简称网络监测平台），使用网络监测平台完善线上反洗钱监管机制、加强信息共享。

中国互联网金融协会按照中国人民银行和国务院有关金融监督管理机构的要求建设、运行和维护网络监测平台，确保网络监测平台及相关信息、数据和资料的安全、保密、完整。

中国人民银行分支机构、中国反洗钱监测分析中心在职责范围内使用网络监测平台。

第六条　金融机构、非银行支付机构以外的其他从业机构应当通过网络监测平台进行反洗钱和反恐怖融资履职登记。

金融机构和非银行支付机构根据反洗钱工作需要接入网络监测平台，参与基于该平台的工作信息交流、技术设施共享、风险评估等工作。

第七条　从业机构应当遵循风险为本方法，根据法律法规和行业规则，建立健全反洗钱和反恐怖融资内部控制制度，强化反洗钱和反恐怖融资合规管理，完善相关风险管理机制。

从业机构应当建立统一的反洗钱和反恐怖融资合规管理政策，对其境内外附属机构、分支机构、事业部的反洗钱和反恐怖融资工作实施统一管理。

从业机构应当按规定方式向中国人民银行及其分支机构、国务院有关金融监督管理机构及其派出机构报备反洗钱和反恐怖融资内部控制制度。

第八条　从业机构应当明确机构董事、高级管理层及部门管理人员的反洗钱和反恐怖融资职责。从业机构的负责人应当对反洗钱和反恐怖融资内部控制制度的有效实施负责。

从业机构应当设立专门部门或者指定内设部门牵头负责反洗钱和反恐怖融资管理工作。各业务条线（部门）应当承担反洗钱和反恐怖融资工作的直接责任，并指定人员负责反洗钱和反恐怖融资工作。从业机构应当确保反洗钱和反恐怖融资管理部门及反洗钱和反恐怖融资工作人员具备有效履职所需的授权、资源和独立性。

第九条　从业机构及其员工对依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息应当予以保密。非依法律规定，不得向任何单位和个人提供。

从业机构及其员工应当对报告可疑交易、配合中国人民银行及其分支机构开展反洗钱调查等有关反洗钱和反恐怖融资工作信息予以保密，不得违反规定向任何单位和个人提供。

第十条　从业机构应当勤勉尽责，执行客户身份识别制度，遵循“了解你的客户”原则，针对具有不同洗钱或者恐怖融资风险特征的客户、业务关系或者交易采取合理措施，了解建立业务关系的目的和意图，了解非自然人客户的受益所有人情况，了解自然人客户的交易是否为本人操作和交易的实际受益人。

从业机构应当按照法律法规、规章、规范性文件和行业规则，收集必备要素信息，利用从可靠途径、以可靠方式获取的信息或数据，采取合理措施识别、核验客户真实身份，确定并适时调整客户风险等级。对于先前获得的客户身份资料存疑的，应当重新识别客户身份。

从业机构应当采取持续的客户身份识别措施，审核客户身份资料和交易记录，及时更新客户身份识别相关的证明文件、数据和信息，确保客户正在进行的交易与从业机构所掌握的客户资料、客户业务、风险状况等匹配。对于高风险客户，从业机构应当采取合理措施了解其资金来源，提高审核频率。

除本办法和行业规则规定的必备要素信息外，从业机构应当在法律法规、规章、规范性文件允许的范围内收集其他相关信息、数据和资料，合理运用技术手段和理论方法进行分析，核验客户真实身份。

客户属于外国政要、国际组织的高级管理人员及其特定关系人的，从业机构应当采取更为严格的客户身份识别措施。

从业机构不得为身份不明或者拒绝身份查验的客户提供服务或者与其进行交易，不得为客户开立匿名账户或者假名账户， 不得与明显具有非法目的的客户建立业务关系。

第十一条　从业机构应当定期或者在业务模式、交易方式发生重大变化、拓展新的业务领域、洗钱和恐怖融资风险状况发生较大变化时，评估客户身份识别措施的有效性，并及时予以完善。

第十二条　从业机构在与客户建立业务关系或者开展法律法规、规章、规范性文件和行业规则规定的特定类型交易时，应当履行以下客户身份识别程序：

（一）了解并采取合理措施获取客户与其建立业务关系或者进行交易的目的和意图。

（二）核对客户有效身份证件或者其他身份证明文件，或者按照法律法规、规章、规范性文件和行业规则要求客户提供资料并通过合法、安全、可信的渠道取得客户身份确认信息，识别客户、账户持有人及交易操作人员的身份。

（三）按照法律法规、规章、规范性文件和行业规则通过合法、安全且信息来源独立的外部渠道验证客户、账户持有人及交易操作人员的身份信息，并确保外部渠道反馈的验证信息与被验证信息之间具有一致性和唯一对应性。

（四）按照法律法规、规章、规范性文件和行业规则登记并保存客户、账户持有人及交易操作人员的身份基本信息。

（五）按照法律法规、规章、规范性文件和行业规则保存客户有效身份证件或者其他身份证明文件的影印件或者复印件，或者渠道反馈的客户身份确认信息。

第十三条　从业机构应当提示客户如实披露他人代办业务或者员工经办业务的情况，确认代理关系或者授权经办业务指令的真实性，并按照本办法第十二条的有关要求对代理人和业务经办人采取客户身份识别措施。

第十四条　从业机构应当执行大额交易和可疑交易报告制度，制定报告操作规程，对本机构的大额交易和可疑交易报告工作做出统一要求。金融机构、非银行支付机构以外的其他从业机构应当由总部或者总部指定的一个机构通过网络监测平台提交全公司的大额交易和可疑交易报告。

中国反洗钱监测分析中心发现从业机构报送的大额交易报告或者可疑交易报告内容要素不全或者存在错误的，可以向提交报告的从业机构发出补正通知，从业机构应当在接到补正通知之日起 5 个工作日内补正。

大额交易和可疑交易报告的要素内容、报告格式和填写要求等由中国人民银行另行规定。

第十五条　从业机构应当建立健全大额交易和可疑交易监测系统，以客户为基本单位开展资金交易的监测分析，对客户及其所有业务、交易及其过程开展监测和分析。

第十六条　客户当日单笔或者累计交易人民币 5 万元以上（含 5 万元）、外币等值 1 万美元以上（含 1 万美元）的现金收支，金融机构、非银行支付机构以外的从业机构应当在交易发生后的 5 个工作日内提交大额交易报告。

中国人民银行根据需要调整大额交易报告标准。非银行支付机构提交大额交易报告的具体要求由中国人民银行另行规定。

第十七条　从业机构发现或者有合理理由怀疑客户及其行为、客户的资金或者其他资产、客户的交易或者试图进行的交易与洗钱、恐怖融资等犯罪活动相关的，不论所涉资金金额或者资产价值大小，应当按本机构可疑交易报告内部操作规程确认为可疑交易后，及时提交可疑交易报告。

第十八条　从业机构应当按照中国人民银行、国务院有关金融监督管理机构的要求和行业规则，建立交易监测标准和客户行为监测方案，定期或者在发生特定风险时评估交易监测标准和客户行为监测方案的有效性，并及时予以完善。

从业机构应当按照法律法规、规章、规范性文件和行业规则，结合对相关联的客户、账户持有人、交易操作人员的身份识别情况，对通过交易监测标准筛选出的交易进行分析判断，记录分析过程；不作为可疑交易报告的，应当记录分析排除的合理理由；确认为可疑交易的，应当在可疑交易报告理由中完整记录对客户身份特征、交易特征或者行为特征的分析过程。

第十九条　从业机构应当对下列恐怖组织和恐怖活动人员名单开展实时监测，有合理理由怀疑客户或者其交易对手、资金或者其他资产与名单相关的，应当立即提交可疑交易报告，并依法对相关资金或者其他资产采取冻结措施：

（一）中国政府发布的或者承认执行的恐怖活动组织及恐怖活动人员名单。

（二）联合国安理会决议中所列的恐怖活动组织及恐怖活动人员名单。

（三）中国人民银行及国务院有关金融监督管理机构要求关注的其他涉嫌恐怖活动的组织及人员名单。

对于新发布或者新调整的名单，从业机构应当立即开展回溯性调查，按照本条第一款规定提交可疑交易报告。对于中国人民银行或者其他有权部门要求纳入反洗钱、反恐怖融资监控体系的名单，从业机构应当参照本办法相关规定执行。

法律法规、规章和中国人民银行对上述名单的监控另有规定的，从其规定。

第二十条　从业机构应当按照法律法规和行业规则规定的保存范围、保存期限、技术标准，妥善保存开展客户身份识别、交易监测分析、大额交易报告和可疑交易报告等反洗钱和反恐怖融资工作所产生的信息、数据和资料，确保能够完整重现每笔交易，确保相关工作可追溯。

从业机构终止业务活动时，应当按照相关行业主管部门及中国人民银行要求处理前款所述信息、数据和资料。

第二十一条　从业机构应当依法接受中国人民银行及其分支机构的反洗钱和反恐怖融资的现场检查、非现场监管和反洗钱调查，按照中国人民银行及其分支机构的要求提供相关信息、数据和资料，对所提供的信息、数据和资料的真实性、准确性、完整性负责，不得拒绝、阻挠、逃避监督检查和反洗钱调查，不得谎报、隐匿、销毁相关信息、数据和资料。金融机构、非银行支付机构以外的其他从业机构通过网络监测平台向中国人民银行报送反洗钱和反恐怖融资报告、报表及相关信息、数据和资料。

从业机构应当依法配合国务院有关金融监督管理机构及其派出机构的监督管理。

第二十二条　从业机构违反本办法的，由中国人民银行及其分支机构、国务院有关金融监督管理机构及其派出机构责令限期整改，依法予以处罚。

从业机构违反相关法律、行政法规、规章以及本办法规定，涉嫌犯罪的，移送司法机关依法追究刑事责任。

第二十三条　本办法相关用语含义如下：

中国人民银行分支机构，包括中国人民银行上海总部、分行、营业管理部、省会（首

府）城市中心支行、副省级城市中心支行。

金融机构是指依法设立的从事金融业务的政策性银行、商业银行、农村合作银行、农村信用社、村镇银行、证券公司、期货公司、基金管理公司、保险公司、保险资产管理公司、保险专业代理公司、保险经纪公司、信托公司、金融资产管理公司、企业集团财务公司、金融租赁公司、汽车金融公司、消费金融公司、货币经纪公司、贷款公司以及中国人民银行确定并公布的从事金融业务的其他机构。

非银行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、数字电视支付等网络支付业务的非银行机构。

行业规则是指由中国互联网金融协会协调其他行业自律组织，根据风险防控需要和业务发展状况，组织从业机构制定或调整，报中国人民银行、国务院有关金融监督管理机构批准后公布施行的反洗钱和反恐怖融资工作规则及相关业务、技术标准。

第二十四条　本办法由中国人民银行会同国务院有关金融监督管理机构负责解释。

第二十五条　本办法自 2019 年 1 月 1 日起施行。

金融信息服务管理规定

基本信息：

【发布机关】中共中央网络安全和信息化委员会办公室、国家互联网信息办公室

【发文字号】-

【发布日期】2018.12.26

【时效性】现行有效

【效力级别】规范性文件

【实施日期】2019.2.1

金融信息服务管理规定

第一条为加强金融信息服务内容管理，提高金融信息服务质量，促进金融信息服务健康有序发展，保护自然人、法人和非法人组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条在中华人民共和国境内从事金融信息服务，应当遵守本规定。

本规定所称金融信息服务，是指向从事金融分析、金融交易、金融决策或者其他金融活动的用户提供可能影响金融市场的信息和/或者金融数据的服务。该服务不同于通讯社服务。

第三条国家互联网信息办公室负责全国金融信息服务的监督管理执法工作，地方互联

网信息办公室依据职责负责本行政区域内的金融信息服务的监督管理执法工作。

第四条金融信息服务提供者从事互联网新闻信息服务、法定特许或者应予以备案的金融业务应当取得相应资质，并接受有关主管部门的监督管理。

第五条金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员，建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范。

第六条金融信息服务提供者应当在显著位置准确无误注明信息来源，并确保文字、图像、视频、音频等形式的金融信息来源可追溯。

第七条金融信息服务提供者应当配备相关专业人员，负责金融信息内容的审核，确保金融信息真实、客观、合法。

第八条金融信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

（一）散布虚假金融信息，危害国家金融安全以及社会稳定的；

（二）歪曲国家财政货币政策、金融管理政策，扰乱经济秩序、损害国家利益的；

（三）教唆他人商业欺诈或经济犯罪，造成社会影响的；

（四）虚构证券、基金、期货、外汇等金融市场事件或新闻的；

（五）宣传有关主管部门禁止的金融产品与服务的；

（六）法律、法规和规章禁止的其他内容。

第九条金融信息服务提供者应当自觉接受用户监督，设置便捷投诉窗口，及时妥善处理投诉事宜，并保存有关记录。

第十条金融信息服务使用者发现金融信息服务提供者所提供的金融信息含有本规定第八条所列内容的，可以向国家或地方互联网信息办公室举报。

第十一条金融信息服务提供者发现含有本规定第八条所列信息内容的，应当立即终止传输、禁止使用和停止传播该信息内容，及时采取处置措施，消除相关信息内容，保存完整记录并向国家或地方互联网信息办公室报告。

第十二条国家和地方互联网信息办公室应当建立日常检查和定期检查相结合的监督管理制度，依法对金融信息服务活动实施监督检查，有关单位、个人应当予以配合。

第十三条金融信息服务使用者向社会传播金融信息服务提供者提供的金融信息中含有本规定第八条所列内容的，由国家或地方互联网信息办公室以及有关主管部门依法处罚。

第十四条金融信息服务提供者违反本规定第五条、第六条、第七条、第八条、第九条规定的，由国家或地方互联网信息办公室依据职责进行约谈、公开谴责、责令改正、列入

失信名单；依法应当予以行政处罚的，由国家或地方互联网信息办公室等有关主管部门给予行政处罚；构成犯罪的，依法追究刑事责任。

第十五条国家和地方互联网信息办公室根据工作需要，与有关主管部门建立金融信息服务情况通报、信息共享等工作机制，对违法违规行为实施联合惩戒。

第十六条鼓励金融信息服务提供者建立行业自律组织，制定服务规范，推动行业信用体系建设，促进行业健康有序发展。

第十七条本规定自 2019 年 2 月 1 日起施行。

互联网个人信息安全保护指南

基本信息：	
【发布机关】公安部	【时效性】 现行有效
【发文字号】-	【效力级别】部门规范性文件
【发布日期】2019.04.10	【实施日期】2019.04.10

互联网个人信息安全保护指南

引 言

为有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会和公安部第三研究所等单位相关专家，研究起草了《互联网个人信息安全保护指南》，供互联网服务单位在个人信息保护工作中参考借鉴。

1 范围

本文件制定了个人信息安全保护的管理机制、安全技术措施和业务流程。

适用于个人信息持有者在个人信息生命周期处理过程中开展安全保护工作参考使用。本文件适用于通过互联网提供服务的企业，也适用于使用专网或非联网环境控制和处理个人信息的组织或个人。

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 25069-2010 信息安全技术 术语

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求（信息系统安全等级保护基本要求）

3 术语和定义

3.1 个人信息

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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

[中华人民共和国网络安全法，第七十六条（五）]

注：个人信息还包括通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

3.2 个人信息主体

个人信息所标识的自然人。

[GB/T 35273-2017，定义 3.3]

3.3 个人信息持有

对个人信息及相关资源、环境、管理体系等进行计划、组织、协调、控制的相关活动或行为。

3.4 个人信息持有者

对个人信息进行控制和处理的组织或个人。

3.5 个人信息收集

获得对个人信息的控制权的行为，包括由个人信息主体主动提供、通过与个人信息主体交互或记录个人信息主体行为等自动采集，以及通过共享、转让、搜集公开信息间接获取等方式。

[GB/T 35273-2017，定义 3.5]

3.6 个人信息使用

通过自动或非自动方式对个人信息进行操作，例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。

3.7 个人信息删除

在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

[GB/T 35273-2017，定义 3.9]

3.8　个人信息生命周期

包括个人信息持有者收集、保存、应用、委托处理、共享、转让和公开披露、删除个人信息在内的全部生命历程。

3.9　个人信息处理系统

处理个人信息的计算机信息系统，涉及个人信息生命周期一个或多个阶段（收集、保存、应用、委托处理、共享、转让和公开披露、删除）。

4　管理机制

4.1　基本要求

个人信息处理系统的安全管理要求应满足 GB/T 22239 相应等级的要求。

4.2　管理制度

4.2.1　管理制度内容

a）应制定个人信息保护的总体方针和安全策略等相关规章制度和文件，其中包括本机构的个人信息保护工作的目标、范围、原则和安全框架等相关说明；

b）应制定工作人员对个人信息日常管理的操作规程；

c）应建立个人信息管理制度体系，其中包括安全策略、管理制度、操作规程和记录表单；

d）应制定个人信息安全事件应急预案。

4.2.2　管理制度制定发布

a）应指定专门的部门或人员负责安全管理制度的制定；

b）应明确安全管理制度的制定程序和发布方式，对制定的安全管理制度进行论证和审定，并形成论证和评审记录；

c）应明确管理制度的发布范围，并对发文及确认情况进行登记记录。

4.2.3　管理制度执行落实

a）应对相关制度执行情况进行审批登记；

b）应保存记录文件，确保实际工作流程与相关的管理制度内容相同；

c）应定期汇报总结管理制度执行情况。

4.2.4　管理制度评审改进

a）应定期对安全管理制度进行评审，存在不足或需要改进的予以修订；

b）安全管理制度评审应形成记录，如果对制度做过修订，应更新所有下发的相关安全管理制度。

4.3　管理机构

4.3.1　管理机构的岗位设置

a）应设置指导和管理个人信息保护的工作机构，明确定义机构的职责；

b）应由最高管理者或授权专人负责个人信息保护的工作；

c）应明确设置安全主管、安全管理各个方面的负责人，设立审计管理员和安全管理员等岗位，清晰、明确定义其职责范围。

4.3.2　管理机构的人员配置

a）应明确安全管理岗位人员的配备，包括数量、专职还是兼职情况等；配备负责数据保护的专门人员；

b）应建立安全管理岗位人员信息表，登记机房管理员、系统管理员、数据库管理员、网络管理员、审计管理员、安全管理员等重要岗位人员的信息，审计管理员和安全管理员不应兼任网络管理员、系统管理员、数据库管理员、数据操作员等岗位。

4.4　管理人员

4.4.1　管理人员的录用

a）应设立专门的部门或人员负责人员的录用工作；

b）应明确人员录用时对人员的条件要求，对被录用人的身份、背景和专业资格进行审查，对技术人员的技术技能进行考核；

c）录用后应签署相应的针对个人信息的保密协议；

d）应建立管理文档，说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；

e）应记录录用人身份、背景和专业资格等，记录审查内容和审查结果等；

f）应记录录用人录用时的技能考核文档或记录，记录考核内容和考核结果等；

g）应签订保密协议，其中包括保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

4.4.2　管理人员的离岗

a）人员离岗时应办理调离手续，签署调离后个人信息保密义务的承诺书，防范内部员工、管理员因工作原因非法持有、披露和使用个人信息；

b）应对即将离岗人员具有控制方法，及时终止离岗人员的所有访问权限，取回其身份认证的配件，诸如身份证件、钥匙、徽章以及机构提供的软硬件设备；采用生理特征进行访问控制的，需要及时删除生理特征录入的相关信息；

c）应形成对离岗人员的安全处理记录（如交还身份证件、设备等的登记记录）；

d）应具有按照离职程序办理调离手续的记录。

4.4.3　管理人员的考核

a）应设立专人负责定期对接触个人信息数据工作的工作人员进行全面、严格的安全审查、意识考核和技能考核；

b）应按照考核周期形成考核文档，被考核人员应包括各个岗位的人员；

c）应对违反违背制定的安全策略和规定的人员进行惩戒；

d）应定期考查安全管理员、系统管理员和网络管理员其对工作相关的信息安全基础知识、安全责任和惩戒措施、相关法律法规等的理解程度，并对考核记录进行记录存档。

4.4.4　管理人员的教育培训

a）应制定培训计划并按计划对各岗位员工进行基本的安全意识教育培训和岗位技能培训；

b）应制定安全教育和培训计划文档，明确培训方式、培训对象、培训内容、培训时间和地点等，培训内容包含信息安全基础知识、岗位操作规程等；

c）应形成安全教育和培训记录，记录包含培训人员、培训内容、培训结果等。

4.4.5　外部人员访问

a）应建立关于物理环境的外部人员访问的安全措施：

1）制定外部人员允许访问的设备、区域和信息的规定；

2）外部人员访问前需要提出书面申请并获得批准；

3）外部人员访问被批准后应有专人全程陪同或监督，并进行全程监控录像；

4）外部人员访问情况应登记备案。

b）应建立关于网络通道的外部人员访问的安全措施：

1）制定外部人员允许接入受控网络访问系统的规定；

2）外部人员访问前需要提出书面申请并获得批准；

3）外部人员访问时应进行身份认证；

4）应根据外部访问人员的身份划分不同的访问权限和访问内容；

5）应对外部访问人员的访问时间进行限制；

6）对外部访问人员对个人信息的操作进行记录。

5　技术措施

5.1　基本要求

个人信息处理系统其安全技术措施应满足 GB/T 22239 相应等级的要求，按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

5.2　通用要求

5.2.1　通信网络安全

5.2.1.1　网络架构

a）应为个人信息处理系统所处网络划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

b）个人信息处理系统应作为重点区域部署，并设有边界防护措施。

5.2.1.2　通信传输

a）应采用校验技术或密码技术保证通信过程中个人信息的完整性；

b）应采用密码技术保证通信过程中个人信息字段或整个报文的保密性。

5.2.2　区域边界安全

5.2.2.1　边界防护

a）应对跨越边界访问通信信息进行有效防护；

b）应对非授权设备跨越边界行为进行检查或限制。

5.2.2.2　访问控制

应在个人信息处理系统边界根据访问控制策略设置访问控制规则。

5.2.2.3　入侵防范

应在个人信息处理系统边界部署入侵防护措施，检测、防止或限制从外部、内部发起的网络攻击行为。

5.2.2.4　恶意代码防范

应在个人信息处理系统的网络边界处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

5.2.2.5　安全审计

a）应在个人信息处理系统的网络边界、重要网络节点进行安全审计，审计应覆盖到每个用户、用户行为和安全事件；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功，以及个人信息的范围、类型、操作方式、操作人、流转双方及其他与审计相关的信息；

c）应对审计记录进行保护，定期备份并避免受到未预期的删除、修改或覆盖等；

d）审计记录的留存时间应符合法律法规的要求；

e）应能够对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

5.2.3　计算环境安全

5.2.3.1　身份鉴别

a）应对登录个人信息处理系统的用户进行身份标识和鉴别，身份鉴别标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b）个人信息处理系统应启用登录失败处理功能，采取诸如结束会话、限制非法登录次数和自动退出等措施；

c）个人信息处理系统进行远程管理时，应采取措施防止身份鉴别信息在网络传输过程中被窃听；

d）个人信息处理系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现，密码技术应符合国家密码主管部门规范。

5.2.3.2　访问控制

a）应对登录个人信息处理系统的用户分配账户和权限；

b）个人信息处理系统应重命名或删除默认账户，修改默认账户的默认口令；

c）个人信息处理系统应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d）个人信息处理系统应进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；

e）个人信息处理系统应由授权主体配置访问控制策略，访问控制策略应规定主体对客

体的访问规则；

f）个人信息处理系统的访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

g）个人信息处理系统应对个人信息设置安全标记，并控制主体对有安全标记资源的访问。

5.2.3.3　安全审计

a）个人信息处理系统应启用安全审计功能，并且审计覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c）应对审计记录进行保护，进行定期备份并避免受到未预期的删除、修改或覆盖等；

d）审计记录的留存时间应符合法律法规的要求；

e）应对审计进程进行保护，防止未经授权的中断。

5.2.3.4　入侵防范

a）个人信息处理系统应遵循最小安装的原则，只安装需要的组件和应用程序；

b）个人信息处理系统应关闭不需要的系统服务、默认共享和高危端口；

c）个人信息处理系统应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

d）个人信息处理系统应能够发现存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

e）个人信息处理系统应能够检测到对重要节点的入侵行为并进行防御，并在发生严重入侵事件时提供报警；

5.2.3.5　恶意代码防范和程序可信执行

应采取免受恶意代码攻击的技术措施或可信验证机制对系统程序、应用程序和重要配置文件/参数进行可信执行验证，并在检测到其完整性受到破坏时采取恢复措施。

5.2.3.6　资源控制

a）应限制单个用户或进程对个人信息处理和存储设备系统资源的最大使用限度；

b）应提供重要节点设备的硬件冗余，保证系统的可用性；

c）应对重要节点进行监视，包括监视 CPU、硬盘、内存等资源的使用情况；

d）应能够对重要节点的服务水平降低到预先规定的最小值进行检测和报警。

5.2.4　应用和数据安全

5.2.4.1　身份鉴别

a）个人信息处理系统应对登录的用户进行身份标识和鉴别，该身份标识应具有唯一性，鉴别信息应具有复杂度并要求定期更换；

b）个人信息处理系统应提供并启用登录失败处理功能，并在多次登录后采取必要的保护措施；

c）个人信息处理系统应强制用户首次登录时修改初始口令，当确定信息被泄露后，应提供提示全部用户强制修改密码的功能，在验证确认用户后修改密码；

d）用户身份鉴别信息丢失或失效时，应采取技术措施保证鉴别信息重置过程的安全；

e）应采取静态口令、动态口令、密码技术、生物技术等两种或两种以上的组合鉴别技术对用户进行身份鉴别，且其中一种鉴别技术使用密码技术来实现。

5.2.4.2　访问控制

a）个人信息处理系统应提供访问控制功能，并对登录的用户分配账户和权限；

b）应重命名或删除默认账户，修改默认账户的默认口令；

c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d）应授予不同账户为完成各自承担任务所需的最小权限，在它们之间形成相互制约的关系；

e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

f）访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；

g）个人信息应设置安全标记，控制主体对有安全标记资源的访问。

5.2.4.3　安全审计

a）个人信息处理系统应提供安全审计功能，审计应覆盖到每个用户，应对重要的用户行为和重要的安全事件进行审计；

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c）应对审计记录进行保护，定期备份，并避免受到未预期的删除、修改或覆盖等；

d）审计记录的留存时间应符合法律法规的要求；

e）应对审计进程进行保护，防止未经授权的中断。

5.2.4.4　软件容错

a）应提供个人信息的有效性校验功能，保证通过人机接口输入或通过通信接口输入的内容符合个人信息处理系统设定要求；

b）应能够发现个人信息处理系统软件组件可能存在的已知漏洞，并能够在充分测试评估后及时修补漏洞；

c）应能够在故障发生时，继续提供一部分功能，并能够实施必要的措施。

5.2.4.5　资源控制

a）在通信双方中的一方在一段时间内未做任何响应时，另一方应能够自动结束会话；

b）应对个人信息处理系统的最大并发会话连接数进行限制；

c）应能够对单个用户的多重并发会话进行限制。

5.2.4.6　数据完整性

a）应采取校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据和个人信息；

b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据和个人信息。

5.2.4.7　数据保密性

a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据和个人信息；

b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据和个人信息。

5.2.4.8　数据备份恢复

a）应提供个人信息的本地数据备份与恢复功能，定期对备份数据进行恢复测试，保证数据可用性；

b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；

c）应提供重要数据处理系统的热冗余，保证系统的高可用性。

5.2.4.9　剩余信息保护

a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；

b）应保证存有个人信息的存储空间被释放或重新分配前得到完全清除。

5.3　扩展要求

5.3.1　云计算安全扩展要求

a）应确保个人信息在云计算平台中存储于中国境内，如需出境应遵循国家相关规定；

b）应使用校验技术或密码技术保证虚拟机迁移过程中，个人信息的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

c）应使用密码技术保证虚拟机迁移过程中，个人信息的保密性，防止在迁移过程中的个人信息泄露。

5.3.2　物联网安全扩展要求

物联网感知节点设备采集信息回传应采用密码技术保证通信过程中个人信息的保密性。

6　业务流程

6.1　收集

个人信息的收集行为应满足以下要求：

a）个人信息收集前，应当遵循合法、正当、必要的原则向被收集的个人信息主体公开收集、使用规则，明示收集、使用信息的目的、方式和范围等信息；

b）个人信息收集应获得个人信息主体的同意和授权，不应收集与其提供的服务无关的个人信息，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息；

c）个人信息收集应执行收集前签署的约定和协议，不应超范围收集；

d）不应大规模收集或处理我国公民的种族、民族、政治观点、宗教信仰等敏感数据；

e）个人生物识别信息应仅收集和使用摘要信息，避免收集其原始信息；

f）应确保收集个人信息过程的安全性：

1）收集个人信息之前，应有对被收集人进行身份认证的机制，该身份认证机制应具有相应安全性；

2）收集个人信息时，信息在传输过程中应进行加密等保护处理；

3）收集个人信息的系统应落实网络安全等级保护要求；

4）收集个人信息时应有对收集内容进行安全检测和过滤的机制，防止非法内容提交。

6.2　保存

个人信息的保存行为应满足以下要求：

a）在境内运营中收集和产生的个人信息应在境内存储，如需出境应遵循国家相关规定；

b）收集到的个人信息应采取相应的安全加密存储等安全措施进行处理；

c）应对保存的个人信息根据收集、使用目的、被收集人授权设置相应的保存时限；

d）应对保存的个人信息在超出设置的时限后予以删除；

e）保存信息的主要设备，应对个人信息数据提供备份和恢复功能，确保数据备份的频率和时间间隔，并使用不少于以下一种备份手段：

1）具有本地数据备份功能；

2）将备份介质进行场外存放；

3）具有异地数据备份功能。

6.3　应用

个人信息的应用应满足以下要求：

a）对个人信息的应用，应符合与个人信息主体签署的相关协议和规定，不应超范围应用个人信息；

注：经过处理无法识别特定个人且不能复原的个人信息数据，可以超出与信息主体签署的相关使用协议和约定，但应提供适当的保护措施进行保护。

b）个人信息主体应拥有控制本人信息的权限，包括：

1）允许对本人信息的访问；

2）允许通过适当方法对本人信息的修改或删除，包括纠正不准确和不完整的数据，并保证修改后的本人信息具备真实性和有效性；

c）完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利；如应用于征信服务、行政司法决策等可能对用户带来法律后果的增值应用，或跨网络运营者使用，应经用户明确授权方可使用其数据；

d）应对个人信息的接触者设置相应的访问控制措施，包括：

1）对被授权访问个人信息数据的工作人员按照最小授权的原则，只能访问最少够用的信息，只具有完成职责所需的最少的数据操作权限；

2）对个人信息的重要操作设置内部审批流程，如批量修改、拷贝、下载等；

3）对特定人员超限制处理个人信息时配置相应的责任人或负责机构进行审批，并对这种行为进行记录。

e）应对必须要通过界面（如显示屏幕、纸面）展示的个人信息进行去标识化的处理。

6.4　删除

a）个人信息在超过保存时限之后应进行删除，经过处理无法识别特定个人且不能复原

的除外；

b）个人信息持有者如有违反法律、行政法规的规定或者双方的约定收集、使用其个人信息时，个人信息主体要求删除其个人信息的，应采取措施予以删除；

c）个人信息相关存储设备，将存储的个人信息数据进行删除之后应采取措施防止通过技术手段恢复；

d）对存储过个人信息的设备在进行新信息的存储时，应将之前的内容全部进行删除；

e）废弃存储设备，应在进行删除后再进行处理。

6.5　第三方委托处理

a）在对个人信息委托处理时，不应超出该信息主体授权同意的范围；

b）在对个人信息的相关处理进行委托时，应对委托行为进行个人信息安全影响评估；

c）对个人信息进行委托处理时，应签订相关协议要求受托方符合本文件；

d）应向受托方进行对个人信息数据的使用和访问的授权；

e）受托方对个人信息的相关数据进行处理完成之后，应对存储的个人信息数据的内容进行删除。

6.6　共享和转让

个人信息原则上不得共享、转让。如存在个人信息共享和转让行为时，应满足以下要求：

a）共享和转让行为应经过合法性、必要性评估；

b）在对个人信息进行共享和转让时应进行个人信息安全影响评估，应对受让方的数据安全能力进行评估确保受让方具备足够的数据安全能力，并按照评估结果采取有效的保护个人信息主体的措施；

c）在共享、转让前应向个人信息主体告知转让该信息的目的、规模、公开范围数据接收方的类型等信息；

d）在共享、转让前应得到个人信息主体的授权同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

e）应记录共享、转让信息内容，将共享、转让情况中包括共享、转让的日期、数据量、目的和数据接收方的基本情况在内的信息进行登记；

f）在共享、转让后应了解接收方对个人信息的保存、使用情况和个人信息主体的权利，

例如访问、更正、删除、注销等；

g）当个人信息持有者发生收购、兼并、重组、破产等变更时，个人信息持有者应向个人信息主体告知有关情况，并继续履行原个人信息持有者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意。

6.7　公开披露

个人信息原则上不得公开披露。如经法律授权或具备合理事由确需公开披露时，应充分重视风险，遵守以下要求：

a）事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施；

b）向个人信息主体告知公开披露个人信息的目的、类型，并事先征得个人信息主体明示同意，与国家安全、国防安全、公共安全、公共卫生、重大公共利益或与犯罪侦查、起诉、审判和判决执行等直接相关的情形除外；

c）公开披露个人敏感信息前，除 6.7 b）中告知的内容外，还应向个人信息主体告知涉及的个人敏感信息的内容；

d）准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；

e）承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任；

f）不得公开披露个人生物识别信息和基因、疾病等个人生理信息；

g）不得公开披露我国公民的种族、民族、政治观点、宗教信仰等敏感数据分析结果。

7　应急处置

7.1　应急机制和预案

a）应建立健全网络安全风险评估和应急工作机制，在个人信息处理过程中发生应急事件时具有上报有关主管部门的机制；

b）应制定个人信息安全事件应急预案，包括应急处理流程、事件上报流程等内容；

c）应定期（至少每半年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程，留存应急培训和应急演练记录；

d）应定期对原有的应急预案重新评估，修订完善。

7.2　处置和响应

a）发现网络存在较大安全风险，应采取措施，进行整改，消除隐患；发生安全事件时，

应及时向公安机关报告，协助开展调查和取证工作，尽快消除隐患；

b）发生个人信息安全事件后，应记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

c）应对安全事件造成的影响进行调查和评估，采取技术措施和其他必要措施，消除安全隐患，防止危害扩大；

d）应按《国家网络安全事件应急预案》等相关规定及时上报安全事件，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

e）应将事件的情况告知受影响的个人信息主体，并及时向社会发布与公众有关的警示信息。

中国银保监会监管数据安全管理办法

基本信息：	
【发布机关】中国银行保险监督管理委员会	【时效性】现行有效
	【效力级别】部门规范性文件
【发文字号】银保监发〔2020〕第 43 号	【实施日期】2020.09.23
【发布日期】2020.09.23	

中国银保监会监管数据安全管理办法

第一章 总 则

第一条 为规范银保监会监管数据安全管理工作，提高监管数据安全保护能力，防范监管数据安全风险，依据《中华人民共和国网络安全法》《中华人民共和国银行业监督管理法》《中华人民共和国保险法》《工作秘密管理暂行办法》等法律法规及有关规定，制定本办法。

第二条 本办法所称监管数据是指银保监会在履行监管职责过程中，依法定期采集,经监管信息系统记录、生成和存储的，或经银保监会各业务部门认定的数字、指标、报表、文字等各类信息。

本办法所称监管信息系统是指以满足监管需求为目的开发建设的，具有数据采集、处理、存储等功能的信息系统。

第三条 本办法所称监管数据安全是指监管数据在采集、处理、存储、使用等活动（以

下简称监管数据活动）中，处于可用、完整和可审计状态，未发生泄露、篡改、损毁、丢失或非法使用等情况。

第四条 银保监会及受托机构开展监管数据活动，适用本办法。

本办法所称受托机构是指受银保监会委托或委派，为银保监会提供监管数据采集、处理或存储服务的企事业单位。

第五条 开展监管数据活动，必须遵守相关法律和行政法规。任何单位和个人对在监管数据活动中知悉的国家秘密、工作秘密、商业秘密和个人信息，应当依照相关规定予以保密。

第六条 银保监会建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

第二章 工作职责

第七条 监管数据安全管理实行归口管理，建立统筹协调、分工负责的管理机制。

银保监会统计信息部门是归口管理部门，负责统筹监管数据安全管理工作。银保监会各业务部门负责本部门监管数据安全管理工作。

第八条 归口管理部门具体职责包括：

（一）制定监管数据安全工作规则和管理流程；

（二）制定监管数据安全技术防护措施；

（三）组织实施监管数据安全评估和监督检查。

第九条 各业务部门具体职责包括：

（一）规范本部门监管数据安全使用，明确具体工作要求，落实相关责任；

（二）组织开展本部门监管数据安全管理工作；

（三）协助归口管理部门实施监管数据安全监督检查。

第三章 监管数据采集、存储和加工处理

第十条 监管数据的采集应按照安全、准确、完整和依法合规的原则进行，避免重复、过度采集。

第十一条 监管数据应通过监管工作网或金融专网进行传输。因客观条件限制需要通过物理介质、互联网或其它网络传输的，应经归口管理部门评估同意。

第十二条 监管数据应存储在银保监会机房，并具有完备的备份措施。确有必要存储在

受托机构机房的，应经归口管理部门评估同意。

第十三条 监管数据存储期限、存储介质管理应按照国家和银保监会有关规定执行。

第十四条 监管数据的加工处理应在监管工作权限或受托范围内进行。未经归口管理部门同意，任何单位和个人不得将代码、接口、算法模型和开发工具等接入监管信息系统。

第十五条 监管数据采集、传输、存储、加工处理、转移交换、销毁，以及用于系统开发测试等活动，应根据监管数据类型和管理要求采取分级分类安全技术防护措施。

第四章 监管数据使用

第十六条 监管数据仅限于银保监会履行监管工作职责使用。纪检监察、司法、审计等党政机关为履行工作职责需要使用监管数据时，按照有关规定办理。

第十七条 监管数据的使用行为应通过管理和技术手段确保可追溯。监管数据用于信息系统开发测试以及对外展示时，应经过脱敏处理。

第十八条 使用未公开披露的监管数据，原则上应在不可连接互联网的台式机或笔记本等银保监会工作机中进行。因客观条件限制需采取虚拟专用网络等方式使用监管数据时，应经归口管理部门评估同意。

第十九条 因工作需要下载的监管数据，仅可存储于银保监会的工作机中。承载监管数据的使用介质应妥善保管，防止数据泄露。

第二十条 在使用监管数据过程中产生的加工数据、汇总结果等信息应视同监管数据进行安全管理。

第二十一条 监管数据对外披露应由指定业务部门按照有关规定和流程实施。

第二十二条 各业务部门因工作需要向非党政机关单位、个人提供监管数据时，应充分评估数据安全风险，经本部门主要负责人同意后实施，必要时与对方签订备忘录和保密协议并报归口管理部门备案。

与境外监管机构或国际组织共享监管数据时，应由国际事务部门依照银保监会签署的监管合作谅解备忘录、合作协议等约定或其他有关工作安排进行管理。

法律法规另有规定的，从其规定。

第二十三条 各业务部门因工作需要和系统下线停用监管数据时，应及时对其采取封存或销毁措施。

第五章 监管数据委托服务管理

第二十四条 各业务部门监管数据采集涉及受托机构提供服务时，应事先与归口管理部门沟通并会签同意。受托机构的技术服务方案，应通过归口管理部门的安全评估。技术服

务方案发生变更的，应事先报归口管理部门进行安全评估。

安全评估不通过的，不得开展委托服务或建立委派关系。

第二十五条 为银保监会提供监管数据服务的受托机构，应满足以下基本条件：

（一）具备从事监管数据工作所需系统的自主研发及运维能力；

（二）具备相关信息安全管理资质认证；

（三）拥有自主产权或已签订长期租赁合同的机房；

（四）网络和信息系统具备有效的安全保护和稳定运行措施，三年内未发生网络安全重大事件；

（五）具备有效的监管数据安全管理措施，能够保障银保监会各部门对监管数据的访问和控制；

（六）具有监管数据备份体系、应急组织体系和业务连续性计划。

第二十六条 银保监会通过与受托机构签订协议，确立监管数据委托服务关系。协议应明确服务项目、期限、安全管理责任和终止事由等内容。

银保监会通过委派方式确立监管数据服务关系的，应下达委派任务书。

第二十七条 因有关政策调整导致原委托或委派事项无需继续履行，或发现受托机构监管数据服务出现重大安全问题的，银保监会有权终止委托或委派关系。

委托或委派关系终止时，受托机构应及时、完整地移交监管数据，并销毁因委托或委派事项而获取的监管数据，不得保留相关数据备份等内容。

第六章 监督管理

第二十八条 各业务部门及受托机构应按照监管数据安全工作规则定期开展自查，发现监管数据安全缺陷、漏洞等风险时，应立即采取补救措施。

第二十九条 归口管理部门应定期对各业务部门及受托机构开展监管数据安全管理评估检查工作。

各业务部门及受托机构对于评估和检查中发现的问题应制定整改措施，及时整改，并向归口管理部门报送整改报告。

第三十条 各业务部门及受托机构发生以下监管数据重大安全风险事项时，应立即采取应急处置措施，及时消除安全隐患，防止危害扩大，并于 48 小时内向归口管理部门报告。

（一）监管数据发生泄露或非法使用；

（二）监管数据发生损毁或丢失；

（三）承载监管数据的信息系统或网络发生系统性故障造成服务中断 4 小时以上；

（四）承载监管数据的信息系统或网络遭受非法入侵、发生有害信息或计算机病毒的大规模传播等破坏；

（五）监管数据安全事件引发舆情；

（六）《网络安全重大事件判定指南》列明的其他影响监管数据安全的网络安全重大事件。

辖区发生以上监管数据重大安全风险事项时，各银保监局应立即采取补救措施，并于 48 小时内向银保监会归口管理部门报告。

第三十一条 归口管理部门应建立监管数据安全事件通报工作机制，及时通报监管数据安全事件。

第七章 附 则

第三十二条 涉密监管数据按照国家和银保监会保密管理有关规定进行管理。

第三十三条 各银保监局承担辖区监管数据安全管理责任，参照本办法制定辖区监管数据安全管理办法，明确职责和管理要求，强化监管数据安全保护。

第三十四条 本办法自印发之日起施行。

（五） 地方政府规范性文件

上海市人民政府印发关于促进本市互联网金融产业健康发展若干意见的通知

基本信息：	
【发布机关】上海市人民政府	【时效性】现行有效
【发文字号】沪府发〔2014〕47 号	【效力级别】规范性文件
【发布日期】2014.8.7	【实施日期】2014.8.7

关于促进本市互联网金融产业健康发展的若干意见

互联网金融是基于互联网及移动通信、大数据、云计算、社交平台、搜索引擎等信息技术，实现资金融通、支付、结算等金融相关服务的金融业态，是现有金融体系的进一步完善和普惠金融的重要内容。其表现形式既包括以互联网为主要业务载体的第三方支付，金融产品销售与财富管理，金融资讯与金融门户，金融大数据采掘加工，网络融资与网络融资中介等新兴、新型金融业态；也包括持牌互联网金融机构，以及各类持牌金融机构设立的主要从事互联网金融相关业务的法人机构或功能性总部。为把本市建成互联网金融发展的高地，进一步提升上海国际金融中心的影响力、辐射力、创新力和资源配置能力，推动中国（上海）自由贸易试验区金融改革创新，助力上海打造具有全球影响力的科技创新中心，现就促进本市互联网金融产业健康发展提出如下若干意见：

一、明确指导思想，突出“四个坚持”

（一）坚持服务实体经济，促进产业转型升级。鼓励互联网金融为符合国家及本市产业导向领域的中小微企业和家庭居民提供多样、灵活的金融服务；支持互联网金融与电子商务、现代物流、信息服务、跨境贸易等领域融合发展，促进相关行业转型升级。

（二）坚持鼓励金融创新，形成竞争发展格局。切实转变观念、创新政府管理模式，以更加包容的态度支持互联网金融企业与持牌金融机构在互联网金融领域进行产品创新、技术创新、服务创新、管理创新和模式创新，在细分领域和行业解决方案方面做专、做深、做精、做细，错位竞争、特色发展，持续提升核心技术水平和综合竞争力。

（三）坚持营造发展环境，完善行业基础设施。立足当前、着眼长远，整合现有政策资源，加强人才培育、研究创新、信用体系、法治环境等方面的基础设施建设，着力营造有利于行业健康发展的良好环境。

（四）坚持规范健康发展，切实防范金融风险。坚持底线思维，妥善处理互联网金融创新发展和风险防范的关系，切实加强投资者教育与金融消费者权益保护，引导互联网金融企业合理有序竞争、规范健康发展。

二、加强政策支持，促进集聚发展

（五）鼓励有条件的企业发展互联网金融业务、申请有关业务许可或经营资质。鼓励有条件的企业在本市发起设立以互联网为主要业务载体或以互联网业务为主要服务领域的各类持牌金融机构。支持电子商务平台等大型互联网企业在本市设立小额贷款、融资担保、融资租赁、商业保理等新型金融企业。支持有条件的互联网金融企业依法申请有关金融业务许可或进行有关金融业务备案，申领增值电信业务经营许可等经营资质。允许主要从事互联网金融业务的企业在名称中使用“互联网金融”或“网络金融”字样，并在工商登记等环节提供便利。

（六）加大对互联网金融企业的支持培育力度。对互联网金融领域的新兴业态和创新模式，本市战略性新兴产业发展专项资金、服务业发展引导资金、高新技术成果转化专项资金等财政资金予以重点支持。支持有条件的互联网金融企业进行软件企业、高新技术企业、技术先进型服务企业等方面认定，按照规定享受相关财税优惠政策。

（七）拓宽互联网金融企业融资渠道。充分发挥上海市大学生科技创业基金、上海市创业投资引导基金等政策性基金的助推作用，探索设立主要投向互联网金融领域早期创业企业的创业投资基金和天使投资基金。支持社会资本发起设立互联网金融产业投资基金、并购基金，鼓励各类机构投资有发展潜力的互联网金融企业。支持互联网金融企业在境内外多层次资本市场上市（挂牌）。

（八）支持持牌金融机构向互联网金融领域拓展转型。支持银行业、证券业、保险业持牌金融机构积极开展互联网金融领域的产品和服务创新，提升金融服务广度、深度和能级。对持牌金融机构在沪设立的主要从事互联网金融相关业务的法人机构或功能性总部，市、区县两级政府可根据相关政策给予支持。

（九）鼓励互联网金融企业合理集聚。积极支持有条件的区县、园区结合自身产业定位，建设有特色的互联网金融产业基地（园区），制定有针对性的政策措施，引导互联网金融企业合理集聚。对优秀互联网金融产业基地（园区），市、区县两级政府可给予一定支持。

三、加强基础建设，营造发展环境

（十）吸引集聚互联网金融人才。支持互联网金融企业的高级管理人员和高级技术人才享受本市人才引进政策，在居住证等入沪手续办理方面提供便利。支持作出突出贡献的互联网金融企业高级管理人才和技术人才申报本市有关高级人才项目。支持高等院校、专业机构加强互联网金融领域人才培训，探索开展从业人员资质认证，对有关培训认证费用可给予适当补贴。

（十一）鼓励互联网金融领域研究创新。鼓励互联网金融企业、持牌金融机构、高等院校等开展互联网金融产业理论、标准、技术和产品等方面的研究。支持设立专业化的互联网金融研究机构，打造具有国际、国内影响力的互联网金融论坛。对互联网金融领域的

重要创新成果，支持申报本市金融创新奖。

（十二）加强互联网金融领域信用体系建设。支持互联网金融企业充分利用各类信用信息查询系统，规范信用信息的记录、查询和使用。支持信用服务机构面向互联网金融领域加强信用产品研发和服务创新，建设互联网金融信用信息服务平台。对为互联网金融企业提供专业信用服务的机构，可按照规定给予一定支持。支持市公共信用信息服务平台与互联网金融企业加强合作，促进公共信用信息、金融信用信息、社会信用信息互动共用。

（十三）完善配套支持体系。鼓励持牌金融机构与互联网金融企业在客户资金存管（监管）、渠道营销、风控外包等方面开展深度合作，构建互联网金融产业联盟，促进信息技术手段与金融业务的融合运用。支持设立、发展提供数据存储及备份、云计算共享、大数据挖掘、信息系统及数据中心外包、信息安全维护等基础服务的机构，支持建立互联网金融数据共享交换平台。

（十四）营造良好法治环境。探索开展互联网金融相关领域地方立法研究，加大对互联网金融企业专利、软件、品牌等知识产权的保护力度。充分发挥上海金融法治环境建设联席会议等工作机制的作用，针对互联网金融行业特点，着力营造良好法治环境。

四、强化风险防控，引导规范发展

（十五）严厉打击互联网金融领域各类违法犯罪行为。充分发挥本市金融稳定例会、打击非法金融活动领导小组等工作机制的作用，积极配合中央金融监管部门开展工作，严厉打击互联网金融领域的非法集资、洗钱犯罪、恶意欺诈、虚假广告、违规交易、买卖客户信息等违法犯罪行为。

（十六）引导互联网金融企业增强合规经营意识、提升风险防控能力。引导互联网金融企业明确经营“底线”、政策“红线”，健全风险管理、信息披露、纠纷处理等方面的内控机制。推动互联网金融企业开展客户资金存管（监管）、做实各类准备金账户，切实提升自身风险防控能力。推动互联网金融企业提升信息技术水平与信息安全防护能力，强化对企业金融数据和客户信息的安全保护。

（十七）支持开展行业自律与第三方监测评估。支持建立互联网金融行业协会、联盟，制定自律公约、行业标准，加强对会员企业及其从业人员的职业道德和职业纪律约束。充分发挥第三方机构作用，探索对有关领域互联网金融活动开展监测评估，建立社会力量参与市场监督的工作机制。

（十八）健全互联网金融风险防控与安全保障机制。针对互联网金融特点，探索建立行业风险监测、预警和应急处置机制。配合国家相关部门健全互联网金融领域支付安全、信息安全等方面的监管制度、技术规范及标准体系。加强相关政府部门间的信息共享，完善本市互联网金融企业及其从业人员诚信体系。

（十九）加强投资者教育和金融消费者权益保护。通过电视、广播、报刊、网络等多

种形式，加强互联网金融适当性教育，提高投资者风险意识及产品认知、风险识别能力。畅通互联网金融消费投诉渠道，加强金融消费者权益保护。

五、健全工作机制，完善部门协同

（二十）健全促进本市互联网金融产业健康发展的工作机制。由本市相关部门、中央在沪监管单位参与，建立本市互联网金融产业发展联席会议（以下简称“联席会议”）。联席会议主要职责是跟踪分析互联网金融产业发展的新情况、新问题，积极向国家有关部门争取先行先试政策，研究确定本市互联网金融产业发展的重点领域和政策措施，协调解决互联网金融产业发展中遇到的困难和问题，推动完善互联网金融领域风险防控和应急处置机制。联席会议召集人由市政府分管领导担任，日常事务由市金融办会同市经济信息化委承担。

杭州市人民政府关于推进互联网金融创新发展的指导意见

基本信息：	
【发布机关】杭州市人民政府	【时效性】现行有效
【发文字号】杭政函〔2014〕166号	【效力级别】规范性文件
【发布日期】2014.11.14	【实施日期】2014.12.14

杭州市人民政府

关于推进互联网金融创新发展的指导意见

各区、县（市）人民政府，市政府各部门、各直属单位：

为推进我市全国互联网金融创新中心建设，丰富区域性金融服务中心内涵，完善现代金融服务体系，根据《中共杭州市委关于学习贯彻党的十八届三中全会精神全面深化重点领域关键环节改革的决定》（市委〔2014〕1号）和《中共杭州市委、杭州市人民政府关于加快发展信息经济的若干意见》（市委〔2014〕6号）的精神，特制定本意见。

一、发展目标

顺应金融业发展趋势，坚持市场主导与政府服务、自身发展与服务经济、创新发展与风险防控相结合，创新组织机构、产品服务、体制机制，积极推动互联网金融产业全面发展，力争到2020年，规划和建设一批具有全国影响力的互联网金融集聚区（含产业园、孵化器、专业楼宇，下同），构建和运作一批具有全国辐射力的互联网金融交易服务平台，培育和发展一批具有全国竞争力的互联网金融企业，开发和推广一批全国市场占有率高的互联网金融创新产品，基本建成全国互联网金融创新中心。

二、发展重点

重点培育发展互联网金融机构和五类互联网金融企业，从市级金融服务业专项资金中统筹安排资金，重点用于扶持互联网金融集聚区和基础设施建设、互联网金融企业培育等。鼓励各区、县（市）设立配套专项资金，支持互联网金融产业发展。通过市、区、集聚区三级联动，落实行业准入、人才培养、信用建设等方面的扶持政策，强化行业管理和风险防控，营造宽松、包容的创新创业氛围和良好、有序的行业发展环境。

（一）互联网金融机构。

指经国家金融监管部门批准设立、具有独立法人资格的网络银行、网络保险公司或其他网络金融机构，以及经国家金融监管部门批准，由银行业、证券业、保险业等传统金融机构发起设立的主要从事互联网金融相关业务的功能性总部。

（二）五类互联网金融企业。

1.第三方支付机构：指获得中国人民银行颁发的《支付业务许可证》，依托互联网在收付款人之间转移货币资金的法人非金融机构。

2.网络债权融资企业：指以依托互联网平台开展资金借贷及相关融资中介等金融服务为主要业务的法人企业。

3.网络股权融资企业：指以依托互联网平台开展股权融资及相关融资中介等金融服务为主要业务的法人企业。

4.互联网金融门户：指主要通过运营互联网门户网站提供综合性金融咨询服务，或主要通过运营互联网金融交易服务平台提供综合性金融产品销售与财富管理服务的法人企业。

5.互联网金融后台：指主要通过金融大数据采掘加工提供增值服务或提供互联网金融业务专业技术支撑的法人企业。

三、企业培育

（一）支持互联网金融机构设立发展。

支持符合条件的企业申请互联网金融经营资质，在杭发起设立互联网金融机构，开展互联网金融业务。支持银行业、证券业、保险业等传统金融机构设立从事互联网金融相关业务的法人机构或功能性总部。积极招引外地互联网金融机构来杭发展。对在杭新设立或新迁入的互联网金融机构，按照杭州市金融机构招商政策给予补助，相关高级管理人员按照金融机构招商政策享受落户、子女教育等方面的待遇。

（二）加大互联网金融企业培育力度。

支持符合条件的企业依法申请互联网金融业务许可，在杭发起设立互联网金融企业，开展互联网金融业务。积极招引外地互联网金融企业来杭发展。

对在杭各类互联网金融企业，根据其行业特点、规模实力、经营效益等情况，由属地政府认定并视其地方贡献情况给予项目补助。特别重大的互联网金融发展项目，经市、区两级政府认定，由属地政府按“一企一策”的原则在项目推进各方面给予优惠扶持，市政

府将视实际情况予以适当支持。

（三）支持互联网金融企业利用资本市场加快发展。

支持市产业发展引导基金、市创业投资引导基金等政策性基金与境内外知名股权投资机构、金融机构合作，在杭发起设立互联网金融发展专项子基金，重点投向我市初创期、成长期互联网金融企业。支持社会资本在杭发起设立互联网金融产业领域的各类投资基金、并购基金、天使基金，引导金融资源和社会资本加大对我市互联网金融企业的投入力度。

支持互联网金融企业实施股份制改造，鼓励符合条件的互联网金融企业挂牌、上市，并按照《杭州市人民政府关于进一步推动企业利用资本市场加快发展的实施意见》（杭政〔2014〕39号）享受相关扶持政策。

（四）鼓励互联网金融企业创新产品服务。

激发互联网企业创新内在动力，鼓励互联网金融企业以服务实体经济为方向，探索针对小微企业和个人多元化投融资需求开展产品创新、技术创新、服务创新、管理创新和模式创新。支持互联网金融企业申报列为杭州市“雏鹰计划”、“青蓝计划”、“瞪羚计划”等培育对象，鼓励符合条件的互联网金融企业申报软件企业、高新技术企业、技术先进型服务企业等方面认定，按照规定享受相关财税优惠政策。

四、产业集聚

（一）规划建设互联网金融集聚区。

按照“有核无界”的布局原则，重点在西溪谷、钱江新城、未来科技城等地建设互联网金融集聚区，由相关区、县（市）政府牵头制定发展规划和具体行动计划，完善各类配套服务设施，落实商务楼宇等互联网金融企业发展空间。支持民间资本建设互联网金融集聚区，支持符合条件的互联网金融集聚区申报科技型企业孵化器，逐步形成互联网金融“多点集聚”的发展局面。

（二）合力促进互联网金融企业集聚发展。

互联网金融集聚区条件成熟后，可向市政府申请授予市级互联网金融集聚区称号。

市级互联网金融集聚区纳入市级金融服务业专项资金支持对象。市政府根据其实际建设投入和对企业扶持情况，通过转移支付方式，按一定比例给予属地政府一次性资助，最高额度不超过 200 万元，用于支持互联网金融企业集聚发展。

市级互联网金融集聚区应针对互联网金融企业发展需求和各自特色定位，制定扶持政策，采取落户补助、房租补贴等优惠措施，吸引互联网金融企业合理集聚，落实专人管理，促进集聚区健康发展。具体扶持政策由属地政府会同市级互联网金融集聚区制定实施。

五、环境营造

（一）支持互联网金融企业注册登记。

除需国家金融监管部门批准设立的互联网金融机构外，对经区、县（市）政府认定的

互联网金融企业，有关部门应在注册登记等环节提供便利，允许其在工商登记企业名称中使用“互联网金融”或“网络金融”字样，在经营范围中使用“互联网金融服务”字样（由国家金融监管部门核准的金融核心业务除外）。

（二）培育、吸引互联网金融人才。

鼓励互联网金融企业、金融机构和科研机构开展互联网金融学术研究、创新交流合作和培训研讨活动。引导在杭高校培养互联网金融人才，鼓励有条件的市属高校开设互联网金融相关专业和课程，加快培养创新型、复合型、应用型金融人才。吸引互联网金融企业的高级管理人员和高级技术人才来杭发展。经区、县（市）政府认定的互联网金融企业，其符合条件的高级管理人员和高级技术人才可享受杭州市人才引进政策或申报杭州市有关高层次人才项目。

（三）健全互联网金融信用体系。

鼓励、支持设立第三方互联网金融信用信息服务机构或服务平台，加快培育和发展征信机构，加强信用产品研发和服务创新，为互联网企业提供信用信息服务。支持互联网金融信用信息服务机构或服务平台与市公共信用信息服务平台、人民银行征信系统开展合作，促进公共信用信息、互联网金融信用信息、社会信用信息互动共享。推动会计、审计、法律、咨询等中介服务机构发展，为互联网金融企业提供优质、专业的中介服务。

（四）搭建互联网金融行业交流合作平台。

为在杭互联网金融机构、互联网金融企业、相关金融机构、中介服务机构搭建交流合作平台，倡导遵守互联网金融行业经营和风险防范规范，加强与人民银行、各金融监管部门、地方政府及相关部门的互动对接，促进互联网金融行业自律管理、有序发展。

（五）打响杭州互联网金融品牌。

加大互联网金融产业宣传力度，充分发挥在杭互联网金融企业的积极性，鼓励其与国内外知名金融媒体、财经信息平台等开展战略合作，依托具有较大影响力的互联网金融论坛、峰会举办各类研讨、推广活动，打造杭州互联网金融品牌。

六、风险防范

（一）建立互联网金融企业监督管理机制。

落实国家关于互联网金融领域的监管制度和标准规范，会同人民银行和各金融监管部门加强对互联网金融企业的规范管理。依托互联网金融协会加强对互联网金融企业的自律监督。

推动互联网金融企业规范开展客户资金存管，按要求存放和使用备付金等客户资金，促进互联网金融企业提升内控管理水平，防范资金风险。推行互联网金融企业信息报告和披露制度，经区、县（市）政府认定的互联网金融企业应当定期向属地政府报告经营情况和经审计的财务情况，同时按规定向投资者公开披露真实的资金流向和项目情况。

（二）健全互联网金融风险防范处置机制。

会同人民银行和各金融监管部门，加强对消费者、投资者的风险教育，探索建立互联网金融行业风险监测、预警和应急处置机制，严厉打击互联网金融领域的违法犯罪活动，引导互联网金融企业严守政策红线，确保不发生区域性、系统性金融风险。研究第三方监测评估机制，开展金融机构信息系统安全等级保护工作，提升互联网金融企业风险防控和信息安全防护能力，强化对企业金融数据和客户信息的安全保护。

区、县（市）政府为互联网金融企业风险处置的第一责任人，牵头处置辖区内互联网金融企业的金融风险，组织开展互联网金融企业纠纷排解、争议处置和消费者维权等协调工作。

七、工作保障

完善互联网金融产业发展工作机制，由市完善创新金融服务体制机制改革小组（办公室设在市金融办）研究确定全市互联网金融产业发展的重大举措，协调解决互联网金融产业发展中遇到的困难和问题。

本意见自发布之日起 30 日后施行，由市金融办负责牵头组织实施。本意见所涉互联网金融企业认定标准、扶持政策操作规程及申报指引等由市金融办牵头制定实施。

杭州市人民政府

2014 年 11 月 14 日

上海市黄浦区人民政府印发黄浦区关于进一步支持互联网金融发展若干意见的通知

基本信息：	
【发布机关】上海市黄浦区人民政府	【时效性】现行有效
【发文字号】黄府发〔2015〕013 号	【效力级别】规范性文件
【发布日期】2015.8.17	【实施日期】2015.8.17

黄浦区关于进一步支持互联网金融健康发展的若干意见

为贯彻落实国务院《关于积极推进“互联网+”行动指导意见》、中国人民银行等十部委《关于促进互联网金融健康发展的指导意见》，为进一步加快机构集聚，规范行业发展，鼓励金融创新，优化产业生态，继续保持外滩金融创新试验区在互联网金融领域的领先地位，现结合发展实际，在前期政策的基础上提出如下意见：

一是进一步做优做强、推进引导集聚。大力吸引网络银行、网络保险、网络证券等持牌金融机构落户发展，积极鼓励持牌金融机构向互联网金融领域的拓展转型，对上述新设的法人机构或功能性总部给予扶持。全力支持条件成熟的互联网金融企业成为持牌机构，

对获得金融经营许可证的企业给予扶持。支持互联网金融企业申请新金融业务资格、企业资质认定、专项经营许可及相关试点。

二是进一步鼓励业态创新、模式创新和产品创新。支持符合条件的企业参与股权众筹融资试点。引导股权众筹融资中介机构平台规范发展，切实支持小微企业发展，增强股权众筹对大众创新创业的服务能力。在市相关部门的指导下，积极开展股权众筹融资注册登记试点，符合条件的试点企业可在名称和经营范围中使用“股权众筹”字样。遵循负面清单和底线思维原则，对于具有首创特征的互联网金融模式、互联网金融产品服务及其应用予以支持。

三是进一步强化互联网金融的孵化功能。设立 1 亿元的“外滩互联网金融创新引导资金”，积极发挥引导资金对互联网金融的投资的引领作用，优先支持创新创业型互联网金融企业和项目。支持持社会资本发起设立互联网金融产业投资基金。积极引导风险投资基金、私募股权投资基金和产业投资基金、并购基金等各类机构深化与互联网金融企业的合作。支持主要面向互联网金融的各类新型孵化器平台的建设，对经认定的互联网金融孵化器，按照众创空间的标准提供便利服务。

四是进一步支持互联网金融企业融资能力的提升。加大对互联网金融企业的上市辅导培育力度，鼓励符合条件的优质互联网金融企业在主板、创业板、新三板、战略新兴板、科技创新板等境内资本市场上市融资。加强与银行等金融机构的合作、运用贷款贴息、成本补贴、服务奖励等措施，引导金融机构创新信贷产品、探索股权和债权相结合的融资服务。积极支持推动融资担保、知识产权质押融资、信用保险保单融资增信等服务帮助互联网金融企业在合理范围内进行增信。

五是进一步发挥专业园区的优势。在优化现有市级产业基地功能的基础上，推动园区扩容。对产业引导集聚效果显著、服务配套完善、具有典型特色的优秀园区（楼宇）运营管理机构给予扶持。探索在园区设立“互联网金融人才联合实训基地”，探索联合企业、高校、专业机构加强互联网金融领域人才培训，对有关培训费用予以适当支持。

六是进一步加快网络征信及网络知识产权保护工作。积极推动符合条件的互联网金融企业与接入金融信用信息基础数据库。支持信用服务机构面向互联网金融领域的征信产品的研发和创新。鼓励互联网企业依法建立信用信息共享平台和数据共联平台。鼓励互联网金融企业进行商标、品牌、专利、版权等知识产权的运用和保护，切实加强相关网络知识产权和专利执法维权工作，加大对新业态、新模式等创新成果的保护力度。

七是进一步奖励创新、服务创新人才。对互联网金融领域有影响、有潜力的创新项目，积极推荐各级专项资金配套扶持。对于代表性的创新成果，重点支持申报市金融创新奖。设立区金融创新奖，凡获得市级金融创新奖的互联网金融项目自然纳入年度区级金融创新

奖的获奖名单，同时，根据评奖机制，对其他具备实力的互联网金融创新项目、创新人才予以表彰和奖励。进一步加大对互联网金融领域代表人士、领军人才、技术骨干的培养，支持申报各级高级人才项目。

八是进一步加强学术研究体系和外滩金融品牌建设。积极联手金融智库、行业组织、互联网金融企业、持牌金融机构、高等院校加大对互联网金融产业理论、行业标准、管理服务等课题研究的投入。全力支持上海新金融研究院在国内互联网金融研究领域保持领先地位，积极推动中国互联网金融研究中心实体化运作。全力打造外滩互联网金融峰会、外滩国际金融峰会等具有国际、国内影响力的专业化论坛品牌。

九是进一步强化管理服务和金融风险防范。在严守区域金融风险防范底线的基础上，结合金融创新新领域、新模式的探索，改进和完善互联网金融包容式的管理。打通事前、事中、事后的全程管理链条、聚焦监管对接、资本对接，争取更多的先行先试。研究并探索新形势下金融风险防范网络及分级管理工作体系建设，积极引入大数据、会计、法律等协同管理资源，健全互联网金融统计监测制度，推动风险预警与处置模式优化、不断提高金融服务安全性。

十是进一步推进行业自律与消费者保护。全面深化与行业协会、各类专业联盟的合作，加强资源整合与优势互补，共同推进行业自律建设及行业合法权益保护工作。引导企业严格信息披露制度，切实降低互联网金融信息不对称。引导企业不断提升技术安全水平，健全互联网金融个人信息保护。探索建立互联网金融仲裁机构，研究符合互联网金融特点的多元化金融消费纠纷和争端解决机制。探索企业共同出资参与设立“金融消费者专项保护基金”。探索采用政府购买服务的方式，充分利用互联网技术，积极开展投资者教育。

广州市人民政府办公厅关于推进互联网金融产业发展的实施意见

基本信息：

【发布机关】广州市人民政府	【时效性】现行有效
【发文字号】穗府办〔2015〕3号	【效力级别】规范性文件
【发布日期】2015.1.29	【实施日期】2015.1.29

广州市人民政府办公厅关于推进互联网金融产业发展的实施意见

各区、县级市人民政府，市政府各部门、各直属机构：

为深入贯彻落实《中共广州市委广州市人民政府关于全面建设广州区域金融中心的决定》(穗字〔2013〕12号)、《广州市人民政府办公厅关于促进广州市服务业新业态发展的若干措施》(穗府办〔2014〕7号)等文件精神，推进互联网金融产业在我市创新、集聚、规

范发展，抢占金融发展制高点，促进区域金融中心建设，经市人民政府同意，现提出如下实施意见：

一、总体要求

(一)重要意义。近年来，以第三方支付、P2P(点对点)网络贷款、众筹平台等为代表的互联网金融企业，依托大数据、云计算、搜索引擎、社交网络等互联网信息技术，发展迅猛，深刻影响并不断改变中国金融业发展格局。作为国家中心城市、中国移动互联网的起源地、国家电子商务示范城市和在全国具有重要影响力的区域金融中心，广州具有发展互联网金融产业的有利条件和坚实基础。大力发展互联网金融产业，对于完善普惠金融服务体系、打造财富管理中心、提升区域金融中心集聚辐射力、支撑实体经济发展、促进产业转型升级等具有重要意义和作用。

(二)总体思路。紧紧抓住大数据时代中国金融业发展的新机遇，将互联网金融产业作为广州区域金融中心建设新的重要突破口，以更具前瞻性的视野、更富包容性的态度、更有创新性的举措大力推进，始终坚持服务实体经济发展和促进区域金融中心建设的基本原则，积极营造适合互联网金融创新创业的条件和环境，牢牢守住不发生区域性、系统性风险的底线，全面推动互联网金融产业实现快速、健康、创新发展。

(三)发展目标。力争在三年内建成 3 个-5 个各具特色的互联网金融产业基地，集聚一批实力雄厚的互联网金融龙头企业，打造若干个品牌卓越的互联网金融服务平台，将广州建设成为互联网金融业态丰富、运行稳健、创新活跃、服务高效、环境优良，在全国具有重要地位和广泛影响力的互联网金融中心城市。

二、大力发展互联网金融产业

(四)发展第三方支付机构。支持第三方支付机构与金融机构共同搭建安全、高效的在线支付平台，开展在线支付、跨境支付、移动支付、基金销售支付等业务。争取国家金融监管部门支持，引导符合条件、有产业支撑的机构设立更多以网络支付为主营业务的第三方支付机构。支持第三方支付机构通过并购等多种方式做大做强。

(五)发展 P2P 网贷机构。支持 P2P 网贷机构加强信息披露，接受市场和投资者的监督。引导 P2P 网贷机构采取由第三方托管资金、设立风险保障金以及引入第三方担保、基金担保、保险担保主体等措施，健全风险控制体系，规范稳健运营。支持广州地区的企业集团或金融控股集团发起设立 P2P 网贷机构，利用集团资源优势做大做强，完善集团产业链条。支持 P2P 网贷机构明确市场定位，创新产品，加快发展，形成特色与品牌。

(六)发展众筹平台。加大政策扶持力度，引导各类众筹平台在我市集聚发展，大力开展股权众筹、实物众筹等业务。支持各类要素交易平台大力开展众筹业务，完善平台服务功能。支持广州股权交易中心发展“青创板”股权众筹平台，引导各类创业资金进入“青创板”，提高股权众筹对接效率，打造全国青年创业项目和创业企业综合金融服务的知名

品牌。

(七)发展互联网金融机构。支持互联网保险机构开展网络安全、电子商务、网购消费者权益保护、社交网络等与互联网相关的财产保险业务，创新与互联网金融特点相适应的履约保证保险或其他担保模式，大力发展网络健康险。依托大型电商企业在我市设立一批互联网特色小额贷款公司，通过互联网平台、大数据技术开展经营活动，促进电子商务产业加快发展。支持符合条件的各类机构发起设立网络银行、网络保险公司、网络证券公司、网络基金公司等创新型互联网金融机构。

(八)发展互联网金融相关及配套服务机构。创造良好条件，大力支持以互联网为主要业务载体的金融产品销售、金融资讯与金融门户、金融大数据采集、数据存储备份、销售结算等互联网金融相关及配套服务机构加快发展，优化互联网金融发展环境。

(九)引导传统金融机构与互联网融合发展。支持银行、保险机构通过互联网、移动终端等渠道提供金融产品和服务，开展直销业务或探索设立直销银行、保险机构，完善线上线下服务体系。支持证券公司、基金期货公司与大型电商企业、第三方支付机构等合作开展互联网理财业务，开设网上直销平台，推动证券基金行业转型升级。支持金融机构、大型电商企业等设立各类主要从事互联网金融业务的法人机构或功能性总部机构。引导传统金融机构及小额贷款公司、融资性担保公司等民间金融组织与互联网金融企业加强业务合作，做大金融市场规模，完善金融服务体系。

(十)规划建设互联网金融产业基地。支持我市越秀、天河、增城等有条件的区(县级市)依托各自优势选址建设互联网金融产业基地，引导互联网金融企业集聚发展。支持互联网金融产业基地建设大数据存储、宽带基础设施等互联网金融基础设施，向互联网金融企业提供云计算标准接口服务、大数据集中处理标准化服务、金融后台集成服务、金融上下游资源垂直搜索引擎等标准化技术服务或产品。支持互联网金融产业基地依托广州超算中心的信息处理和服务能力开展互联网金融技术创新。

(十一)探索建设广州金融大数据系统。依托政府公共信息平台，整合广州地区大型商业公司、电商企业、银行、小额贷款公司、融资性担保公司、各类要素交易平台、电信、大型社交网站的用户交易记录、支付记录等数据信息，探索建设广州金融大数据系统，为互联网金融发展提供强大的后台支撑。

(十二)成立互联网金融产业联盟服务平台。成立由金融机构、投资机构、互联网金融企业、互联网金融产业基地、金融市场服务机构、互联网金融研究机构、大专院校等参加的广州互联网金融产业联盟服务平台，制定互联网金融行业经营规范标准，加强联盟成员间的沟通交流，实现优势互补、合作共赢、协同创新、规范自律。

三、加大对互联网金融的扶持力度

(十三)支持互联网金融企业注册登记。允许互联网金融企业在工商部门登记企业名称

和经营范围时使用“互联网金融信息服务”或“网络金融信息服务”等内容。

(十四)对互联网金融企业给予一次性落户奖励。互联网金融属于金融新业态范畴，我市互联网金融企业可享受《广州市人民政府关于支持广州区域金融中心建设的若干规定的通知》(穗府〔2013〕11号)的有关扶持政策。对法人机构在广州注册、规模大、经营规范、行业影响力强的互联网金融企业给予一次性落户奖励。企业年利润总额达 1亿元(含)以上的，一次性奖励 1000万元;企业年利润总额 1亿元以下、5000万元(含)以上的，一次性奖励 500万元;企业年利润总额 5000万元以下、2000万元(含)以上的，一次性奖励 200万元;企业年利润总额 2000万元以下、1000万元(含)以上的，一次性奖励 100万元。本实施意见有效期内互联网金融企业只能申请一次落户奖励。

(十五)对互联网金融企业给予业务补贴。法人机构在广州注册、营业收入排名广州地区前 20名的互联网金融企业提供融资或金融服务，如能达到下列条件，则按以下标准给予业务补贴：企业年度营业收入总额达 5000万元以上的，补贴 100万元;企业年度营业收入总额达 2000-5000万元(含)的，补贴 60万元;企业年度营业收入总额达 1000-2000万元(含)的，补贴 30万元;企业年度营业收入总额达 500-1000万元(含)的，补贴 15万元。

(十六)大力培养引进互联网金融人才。对入选广州高层次金融人才的互联网金融人才，按《广州市高层次金融人才支持项目实施办法(试行)》(穗金融〔2014〕83号)的规定给予补贴。对法人机构在广州注册且持续规范经营，年度利润总额达到 1000万元(含)以上的互联网金融企业高级管理人员，可按照《广州市人民政府关于印发支持广州区域金融中心建设的若干规定的通知》(穗府〔2013〕11号)给予每月 1000元住房补贴。

(十七)支持互联网金融项目参评广州市有关金融创新奖励。具有较高创新价值和广泛影响力的互联网金融项目，可根据《广州市人民政府关于印发支持广州区域金融中心建设的若干规定的通知》(穗府〔2013〕11号)参评广州市有关金融创新奖励。

(十八)出台推进互联网金融产业基地建设的政策措施。互联网金融产业基地所在区(县级市)政府应出台扶持政策措施，对在互联网金融产业基地落户的互联网金融企业购买或租赁办公用房、业务发展等给予区(县级市)级财政资金扶持，加快公共基础设施建设，整合楼宇资源，营造促进互联网金融企业集聚发展的良好环境。互联网金融产业基地所在区(县级市)可组织符合条件的项目申请市战略性主导产业发展资金补助。

(十九)支持互联网金融企业多渠道融资。引导社会资本设立互联网金融产业投资基金，对处于种子期、初创期、成长期的互联网金融创新项目加以培育。支持互联网金融企业上市融资和在全国中小企业股份转让系统、广州股权交易中心挂牌交易，支持互联网金融企业发行企业债券、公司债券、短期融资券、中期票据、中小企业私募债等债务融资工具，探索开展资产证券化业务，拓宽资金来源渠道。

四、营造良好的互联网金融发展环境

(二十)完善互联网金融市场环境。加快社会信用体系建设，营造良好的互联网金融发展信用环境，探索推动互联网金融企业接入人民银行征信系统。引导电商企业、互联网金融企业等发起设立互联网金融信用机构，为互联网金融发展提供信用信息服务。引导社会化的创业服务机构为互联网金融企业提供注册设立、融资对接、信用评估、财务核算、业务营销、人才招聘等专业化服务。支持会计、审计、法律、信用评级、担保、咨询等金融市场服务机构为互联网金融企业提供配套服务。

(二十一)优化互联网金融政务与法制环境。工商、税务等部门为互联网金融企业办理注册登记等事项提供优质高效政务服务。支持广州金融仲裁院充分利用仲裁方式解决互联网金融纠纷，研究出台互联网金融仲裁指导意见，形成专门的互联网金融仲裁员队伍。

(二十二)营造互联网金融社会环境。依托广州国际金融研究院，成立广州互联网金融研究中心研究互联网金融重大课题，成立广州互联网金融实训室开展互联网金融实务操作训练。依托广州互联网金融产业联盟服务平台举办互联网金融创新大赛、互联网金融论坛、互联网金融文化沙龙等活动。依托中国(广州)国际金融交易·博览会开展互联网金融宣传、产品营销和文化交流活动。依托广州社区、农村金融服务站开展互联网金融知识进社区、进农村活动。支持互联网金融专著参评全国金融图书“金羊奖”。引导媒体加大对互联网金融的正面宣传力度，营造有利于互联网金融产业发展的舆论环境。

五、建设互联网金融安全运行区

(二十三)强化互联网金融外部监管。按照国家对互联网金融监管的要求，强化各部门之间的协调联动，形成良好的互联网金融监督管理协调合作机制，加强对互联网金融企业的风险监测、预警和处置。严厉打击利用互联网技术或以互联网金融名义开展的非法集资、非法证券、内幕交易、非法外汇、非法支付结算等各类违法犯罪活动。支持国家金融监管部门开展互联网金融法制教育和警示宣传活动，对投资者普及互联网金融知识和开展投资风险教育，增强其对互联网金融的风险防范能力，保护金融消费者的合法权益。

(二十四)加强互联网金融行业自律。充分发挥互联网金融产业联盟服务平台或行业协会等组织的作用，制定自律公约、行业标准，加强会员间的信息交流和行业自律。

(二十五)完善互联网金融企业内部风险防控机制。引导互联网金融企业强化金融风险意识，认真执行国家有关监管规定，借鉴金融机构开展内部风险控制的经验做法，完善法人治理结构，建立健全各项内部管理和风险控制制度，强化信息披露，形成规范经营、稳健发展的互联网金融企业经营文化。

六、保障措施

(二十六)建立互联网金融产业发展部门联席会议。建立由人民银行广州分行营业管理部、广东银监局、广东证监局、广东保监局，市金融办、发展改革委、财政局、经贸委、工商局、科技和信息化局、公安局，各互联网金融产业基地所在区(县级市)政府等组成的

广州互联网金融产业发展部门联席会议，研究广州互联网金融产业发展的重大项目和重大问题，联席会议办公室设在市金融办，如有必要时可提请分管市领导协调。

(二十七)加大财政资金扶持。互联网金融企业可按规定申报我市战略性主导产业发展资金的扶持和奖励。市金融办会同市财政局等单位做好资金的申报、审核、报批和下达资金等工作，具体办法另行制定;互联网金融人才补贴按照高层次人才专项资金要求申报、审核和下达资金。

(二十八)加强人才保障。综合运用政府组团招聘、网络招聘、市场招聘、定向猎取等方式引进一批互联网金融领军人才、高级管理人才和高级专业人才。支持互联网金融产业联盟服务平台等主体在互联网金融产学研等领域加强合作，培育互联网金融人才，开展互联网金融从业人员培训活动，提高从业人员综合素质。支持金融机构或大型互联网金融企业建立互联网金融博士后工作站。

(二十九)推进落实重点项目。明确广州互联网金融产业发展的重点项目和重点工作，建立重点项目储备库，对重点项目和重点工作进行动态管理，实施重点项目责任制和评估机制，确保落实推进。

二、标准

（一）国家标准

1.《信息安全技术 金融信息保护规范》（征求意见稿）

2.《金融服务 信息安全指南》（GB/T 27910—2011）

3.《金融服务 生物特征识别 安全框架》（GB/T 27912—2011）

（二）行业标准

1.《征信机构信息安全规范》（JR/T 0117—2014）

2.《证券期货业数据分类分级指引》（JR/T 0518—2018）

3.《网上银行系统信息安全通用规范》（JR/T 0068—2020）

4.《金融行业网络安全等级保护测评指南》（JR/T 0072—2020）

5.《个人金融信息保护技术规范》（JR/T 0171—2020）

6.《证券期货移动互联网应用程序安全规范》（JR/T 0192—2020）

7.《金融数据安全 数据安全分级指南》（JR/T 0197—2020）

8.《金融科技创新安全通用规范》（JR/T 0199—2020）

9.《金融业数据能力建设指引》（JR/T 0218—2021）

10.《金融数据安全 数据生命周期安全规范》（JR/T 0223—2021）

11.《证券期货业网络安全等级保护基本要求》（JR/T 0060—2021）

12.《证券期货业网络安全等级保护测评要求》（JR/T 0067—2021）

（三）其他

1.《金融服务 生物特征识别安全框架》（ISO 19092:2008）

2.《金融服务 隐私影响评估》（ISO 22307—2008）

3.《金融服务 密码算法及其使用建议》（ISO/TR 14742:2010）

4.《金融服务 个人识别码的管理与安全》（ISO 9564:2017）

5.《金融服务 第三方支付服务供应商》 (ISO/TR 21941:2017)

6.《移动金融服务 第 1 部分：基本框架》 (ISO/TS 12812—1:2017)

7.《移动金融服务 第 2 部分：移动金融服务的安全和数据保护》 (ISO/TS 12812—2:2017)

8.《移动金融服务 第 3 部分：金融应用生命周期管理》 (ISO/TS 12812—3:2017)

9.《移动金融服务 第 4 部分：移动的个人对个人支付》 (ISO/TS 12812—4:2017)

10.《移动金融服务 第 5 部分：移动的个人对企业支付》 (ISO/TS 12812—5:2017)

三、行业案例

（一）司法案例

1. 钟某秀侵犯公民个人信息罪

广东省深圳市宝安区人民法院刑事判决书

（2018）粤 0306 刑初 5473 号

公诉机关：深圳市宝安区人民检察院

被告人：钟某秀

【基本案情】

2017 年 8 月，被告人钟某秀在已离职的深圳 XXX 外汇公司及深圳 XX 互联网金融服务公司上班时基于开发客户的需要，因工作关系获取到 8100 余条包含姓名、联系方式、住址等内容的公民个人信息。被告人钟某秀在职时将上述信息储存在腾讯微云里，离职后从腾讯微云又将公民个人信息下载到自己的 U 盘中，被告人钟某秀使用上述公民个人信息在现就职的深圳市 XX 电子商务公司进行业务推广。2018 年 6 月 14 日 15 时许，被告人钟某秀在深圳市宝安区新桥街道上星社区沙井中心路 XXX 号 XX 大厦被抓获归案，并现场缴获 U 盘一个。

【法院判决】

被告人钟某秀的行为构成侵犯公民个人信息罪，其具有认罪认罚情节。

一、被告人钟某秀犯侵犯公民个人信息罪，判处有期徒刑六个月，缓刑一年，并处罚金人民币八千元（缓刑考验期从判决确定之日起计算。罚金已缴纳）。

二、缴获的作案工具 U 盘一个，依法予以没收。

2. 蓝南信侵犯公民个人信息罪

福建省厦门市中级人民法院刑事判决书

（2018）闽 02 刑终 741 号

公诉机关：厦门市翔安区人民检察院

上诉人（原审被告人）：蓝南信

【基本案情】

被告人蓝南信于 2018 年 1 月起在其位于漳州市漳浦县的住家内从事网络贷款业务，

并于同年 1 月 30 日注册成立厦门壹信云信息科技有限公司，后于同年 3 月 1 日左右将公司搬迁至其租赁的位于厦门市翔安区民房内经营。期间，被告人蓝南信为推广网贷业务，通过ＱＱ群及“借易到”、“云借条”等网络平台非法购买、收受 50684 条包含姓名、联系电话、身份证号码、住址或微信号码、ＱＱ号码、芝麻信用积分等内容的真实公民个人信息。之后，被告人蓝南信通过群发短信方式向非法获取的公民手机号码推送内容为“万三金服，尊敬的ｘｘｘ用户，你的初审已经通过，可用额度为 800-5000 元人民币，请联系官方客服ＱＱ：ｘｘ×××××ｘｘｘｘ”的网贷信息，让对方添加昵称为“万三客服”等的多个公司专用客服ＱＱ号码，并雇请黄某 1、林某、蓝某 1、施某等人负责审核贷款人员资质及办理贷款事宜等，并从中收取贷款金额 40%的手续费。

2018 年 4 月 23 日 11 时许，被告人蓝南信在公安机关对翔安区新店镇陈塘东里 22 号的民房进行清查时被当场抓获，并被现场缴获作案工具电脑主机 7 台、手机 4 部等，归案后对上述犯罪行为供认不讳。

【法院判决】

上诉人蓝南信违反国家有关规定，非法获取公民个人信息共计 50684 条，情节特别严重，其行为已构成侵犯公民个人信息罪。蓝南信接受公安机关盘问时主动交代自己的罪行，到案后能如实供述，可视为自动投案，系自首，依法可以从轻或者减轻处罚。原判未认定上诉人具有自首情节不当，应予纠正。原判定罪准确，证据充分，审判程序合法。鉴于上诉人蓝南信具有自首情节，其获取这些信息并没有违反公民的主观意愿等具体情节，没有再犯罪的危险，社区监管机构也同意对其进行社区矫正，依法可减轻处罚并适用缓刑，原判量刑不当，应予改判。

一、维持厦门市翔安区人民法院（2018）闽 0213 刑初 548 号刑事判决第一项对上诉人蓝南信定罪及第二、三项的判决部分；

二、撤销厦门市翔安区人民法院（2018）闽 0213 刑初 548 号刑事判决第一项对上诉人蓝南信量刑的判决部分；

三、上诉人蓝南信犯侵犯公民个人信息罪，判处有期徒刑二年三个月，缓刑三年，并处罚金人民币二万元。

3. 黄某、朱某等侵犯公民个人信息罪

上海市虹口区人民法院刑事判决书

（2019）沪 0109 刑初 1070 号

公诉机关：上海市虹口区人民检察院

被告人：黄某、朱某、沈某某

【基本案情】

2019 年 8 月至案发，被告人黄某利用在浙江民泰商业银行工作、可以接触到公民产调信息的工作便利，接受徐某某(另案处理)的委托，以每条 50 元左右的价格将从银行中窃取的公民产调信息出售给徐某某。徐某某再将上述信息转手倒卖给邓某某、赵某某(另案处理)以及被告人朱某。被告人朱某将从徐某某处获取的公民产调信息转手倒卖给被告人沈某某，从中赚取每条人民币 10 元左右的差价。被告人沈某某将从朱某处获取的公民产调信息转手倒卖给他人，从中赚取每条人民币 70 元左右的差价。案发后经查，被告人黄某涉案信息 216 条，被告人朱某、沈某某涉案信息均为 60 条(含本市虹口区公民信息)。

2019 年 9 月 25 日被告人朱某经公安机关电话通知，主动至公安机关，如实供述了罪行。2019 年 9 月 25 日被告人黄某、沈某某被公安机关抓获。

【法院判决】

被告人黄某、朱某、沈某某违反国家有关规定，其中被告人黄某以窃取的方法非法获取公民个人信息并向他人出售，被告人朱某、沈某某以购买的方式非法获取公民个人信息并向他人出售，其行为均已构成侵犯公民个人信息罪。上海市虹口区人民检察院指控被告人黄某、朱某、沈某某犯侵犯公民个人信息罪罪名成立。案发后，被告人朱某能自动投案，并能如实供述自己的罪行，系自首，可依法从轻处罚；被告人黄某能如实供述自己的罪行，且在本院审理期间，其家属能主动帮助退缴全部违法所得，并预缴罚金，可依法予以从轻处罚；被告人沈某某能如实供述自己的罪行，可依法予以从轻处罚。

一、被告人黄某犯侵犯公民个人信息罪，判处有期徒刑九个月，并处罚金人民币一万元。

二、被告人朱某犯侵犯公民个人信息罪，判处拘役三个月十日，并处罚金人民币二千元。

三、被告人沈某某犯侵犯公民个人信息罪，判处拘役四个月，并处罚金人民币五千元。

四、违法所得予以没收。

五、缴获的犯罪工具予以没收。

4. 谭某某、吴某某、饶某某侵犯公民个人信息罪

辽宁省抚顺市中级人民法院刑事判决书

（2020）辽 04 刑终 15 号

公诉机关：抚顺市望花区人民检察院

被告人：谭某某、吴某某、饶某某

【基本案情】

被告人谭某某、吴某某、饶某某均系银行工作人员，2017 年 3 月份，谭某某的微信好友付爱军（另案处理）欲向其购买征信信息，谭某某便找到其大学校友吴某某，吴某某找到其负责个贷业务的同事饶某某，三人建立一个微信群，谭某某将付爱军提供的签字授权书等文件照片发至群里，由饶某某查询后发送给谭某某，吴某某、饶某某按条数收取报酬。2017 年 8 月份饶某某退出，后由吴某某亲自查询后发送给谭某某，谭某某将从吴某某、饶某某处购买的征信信息出售给付爱军，从中获利，直至 2017 年 11 月份吴某某退出。

2017 年 4 月份，被告人谭某某与北京融泰安达信息咨询有限公司员工刘某（不起诉）成为微信好友，谭某某从付爱军等人手中购买征信信息出售给刘某，从中获利。

经查证，被告人谭某某侵犯公民征信信息 325 条，被告人吴某某侵犯公民征信信息 234 条，被告人饶某某侵犯公民征信信息 193 条。

【法院判决】

上诉人（原审被告人）谭某某、吴某某、饶某某违反国家有关规定，非法获取、出售公民个人信息，情节严重，其行为均已构成侵犯公民个人信息罪，且系共同犯罪。上诉人谭某某、吴某某、饶某某到案后能如实供述自己的主要罪行，可从轻处罚。

一、撤销抚顺市望花区人民法院（2019）辽 0404 刑初 113 号刑事判决。

二、上诉人（原审被告人）谭某某犯侵犯公民个人信息罪，判处有期徒刑一年四个月，并处罚金人民币三万元（已缴纳）。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押 1 日折抵刑期 1 日，即自 2019 年 11 月 15 日起至 2020 年 9 月 16 日止。已折抵 5 个月 28 日。）

三、上诉人（原审被告人）吴某某犯侵犯公民个人信息罪，判处有期徒刑一年，并处罚金人民币三万元（已缴纳）。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押 1 日折抵刑期 1 日，即自 2019 年 11 月 15 日起至 2020 年 5 月 23 日止。已折抵 5 个月 23 日。）

四、上诉人（原审被告人）饶某某犯侵犯公民个人信息罪，判处有期徒刑十一个月，并处罚金人民币二万元（已缴纳）。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，羁押 1 日折抵刑期 1 日，即自 2019 年 11 月 15 日起至 2020 年 5 月 13 日止。已折抵 5 个月零 1 日。）

五、扣押在案的涉案物品，由扣押机关抚顺市公安局望花公安分局依法处理。

六、上诉人谭某某退缴的违法所得人民币八千元；上诉人吴某某退缴的违法所得人民币一万元；上诉人饶某某退缴的违法所得人民币七千元，依法上缴国库。

5. 熊鹏、谭统权侵犯公民个人信息罪

四川省峨眉山市人民法院刑事判决书

（2020）川 1181 刑初 49 号

公诉机关：四川省峨眉山市人民检察院

被告人：熊鹏、谭统权

【基本案情】

“秒贷吧”APP 软件系银承派公司开发，是一款做借贷业务的产品，通过上架到不同的渠道平台对外放贷，并获取贷款人基本信息、通讯录以及通话记录等。获取信息方式有两种，一是将贷款产品上架到一些渠道平台的贷款超市，用户通过这些渠道平台进行贷款时，贷款超市通过要求用户注册的方式获取用户个人身份信息、电话号码、紧急联系人等基本信息。注册完毕后，客户贷款继续点击相关提示时，贷款超市利用爬虫软件获取贷款人通讯录、通话记录等信息；二是将贷款产品链接嫁接到一些流量平台，用户点击链接下载 APP 后，注册登记，获取客户基本信息，用户继续点击相关提示时，公司利用爬虫软件获取贷款人通讯录、通话记录等信息。

郑某于 2019 年 5 月到银承派公司担任贷后部主管，主要工作内容为：排查系统内逾期未归还的人员名单及信息，物色联系外包催收公司，联络外包催收公司询问催款进度。2019 年 7 月，郑某联系皓城信达公司、金传信用管理（广州）有限公司（以下简称金传公司）进行贷款催收，并将公司逾期未还款的人员信息网站、账户、密码发给上述两家公司法定代表人熊鹏、谭统权，熊鹏、谭统权进一步安排催收事宜。

被告人熊鹏系皓城信达公司法定代表人，后熊某入股，该公司自经营以来一直从事催收工作。公司运作模式为：熊鹏收到郑某发送的催收网址和账号后建立分支账号，并将账号给公司主管人员胡某 1、吕某，由胡某 1、吕某负责将催收名单分配给员工，员工进入公司催收平台，获取贷款人员个人信息（包括逾期贷款人员姓名、身份证号、联系电话、贷款金额、通讯录信息等），员工使用虚拟电话软件给催收号码拨打电话进行催收，如果多次拨打电话后逾期未还款或联系不上客户，则拨打其联系人电话进行催收。

被告人谭统权系金传公司法定代表人，该公司自经营以来一直从事催收工作。公司运作模式为：谭统权收到郑某发送的催收网址和账号后，将催收平台的网址、账号和密码通

过微信发在员工微信群里，由催收人员陈某、肖某 1 等人再进入催收平台，获取贷款人员个人信息（包括逾期贷款人姓名、身份证号、联系电话、贷款金额、通讯录信息等），进行电话催收，如果多次拨打电话后逾期未还款人员仍未还款或联系不上客户，则拨打其联系人电话进行催收。

截止 2019 年 11 月 20 日，皓城信达公司员工胡某 1、钱某 2、方某、吴某、邱某、钱某 1、刘某 4、肖某 2、饶某、严某、王某通过熊鹏提供的催收网址、账号、密码非法获取公民通讯录信息共计 2853111 条；金传公司员工陈某、何某、肖某 1 通过谭统权提供的催收网址、账号、密码非法获取公民通讯录信息共计 242498 条。

【法院判决】

被告人熊鹏、谭统权违反国家规定，使用提供、收受等手段侵犯公民个人信息，情节特别严重，其行为构成侵犯公民个人信息罪。公诉机关的相关指控成立，本院予以支持。被告人熊鹏、谭统权到案后能如实供述自己的罪行，依法可以从轻处罚。被告人熊鹏、谭统权承认指控的犯罪事实，愿意接受处罚，依法对其从宽处理。被告人熊鹏、谭统权的辩护人所提相关辩护意见本院予以采纳。

一、被告人熊鹏犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑四年，并处罚金人民币四万元（已缴纳）；

二、被告人谭统权犯侵犯公民个人信息罪，判处有期徒刑三年，缓刑三年，并处罚金人民币二万元（已缴纳）；

三、从陈某处扣押在案的作案工具电脑主机、录音盒，从谭统权处扣押的作案工具电脑主机、内存条、录音盒、路由器、金色华为手机，从胡某 1 处扣押的作案工具电脑，从熊鹏处扣押的作案工具金色苹果 5 S 手机，依法予以没收，由扣押机关峨眉山市公安局依法处置。

6. 欧阳震勃侵犯公民个人信息罪

广东省佛山市南海区人民法院刑事判决书

(2020)粤 0605 刑初 19 号

公诉机关：佛山市南海区人民检察院

被告人：欧阳震勃（曾用名欧阳勃）

【基本案情】

2015 年 9 月至 11 月份，被告人欧阳震勃在经营利信创通公司（房产和金融贷款中介）

期间，为节省公司费用、提高业绩，先后 11 次向原佛山市*******工作人员邓杰濠（另案处理）非法购买包括各楼盘小区业主姓名、手机号码等的公民个人信息共 52700 余条，其中同年 10 月 29 日前购买的公民个人信息约 5 万条（当中 6600 余条为电话号码，43000 余条包含姓名及电话号码），同年 11 月 12 日、17 日购买的公民个人信息共 2600 余条（均包含姓名及电话号码）。

另查明，民警从被告人欧阳震勃处扣押苹果牌手机一台。

【法院判决】

被告人欧阳震勃以其他方法非法获取公民个人信息，情节严重，其行为已构成非法获取公民个人信息罪。欧阳震勃归案后如实供述自己的罪行，认罪认罚，依法从轻处罚并适用缓刑，采纳辩护人的相关辩护意见。依照经 2009 年《中华人民共和国刑法修正案（七）》修正的《中华人民共和国刑法》第二百五十三条之一第一、二款和《中华人民共和国刑法》第六十七条第三款、第七十二条第一、三款、第七十三条第二、三款、第五十二条、第五十三条之规定，判决如下：

一、被告人欧阳震勃犯非法获取公民个人信息罪，判处有期徒刑一年三个月，缓刑二年，并处罚金人民币二万元（缓刑考验期限，从判决确定之日起计算。罚金从本判决发生法律效力之日起十日内缴纳）。

二、扣押的苹果牌手机一台，发还予被告人欧阳震勃。

（二）执法案例

1. 因个人贷款业务管理漏洞，平安银行被罚 772 万

2020 年 7 月 11 日，京银保监罚决字〔2020〕21 号罚单显示，平安银行北京分行因存在采取不正当手段发放贷款，个人贷款业务内控管理存在多项缺陷，以表外资金掩盖表内承兑汇票垫款等 6 项违法违规行为，被监管处以 772.22 万元处罚，当事员工刘静被禁止 3 年内从事银行业工作。

北京银保监局行政处罚信息公开表

（北京银行城市副中心分行）

行政处罚决定书文号			京银保监罚决字〔2020〕24号
被处罚当事人	个人姓名		——
	单位	名称	北京银行城市副中心分行
		法定代表人（主要负责人）姓名	丁慈秀
主要违法违规事实（案由）			员工行为管理不到位。
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条。
行政处罚决定			责令北京银行城市副中心分行改正，并给予40万元罚款的行政处罚。
作出处罚决定的机关名称			北京银保监局
作出处罚决定的日期			2020年7月11日

2. 因信息系统安全问题，农行被处罚 420 万

2021 年 1 月 19 日，中国银保监会公布的一份行政处罚决定书显示，中国农业银行股份有限公司因信息系统存在安全漏洞等问题被中国银行保险监督管理委员会罚款 420 万元人民币。

中国银行保险监督管理委员会行政处罚信息公开表
（银保监罚决字〔2021〕1号）

（中国农业银行股份有限公司）

行政处罚决定书文号			银保监罚决字〔2021〕1号
被处罚当事人	单位	名称	中国农业银行股份有限公司
		法定代表人姓名	周慕冰
主要违法违规事实（案由）			（一）发生重要信息系统突发事件未报告 （二）制卡数据违规明文留存 （三）生产网络、分行无线互联网络保护不当 （四）数据安全管理较粗放，存在数据泄露风险 （五）网络信息系统存在较多漏洞 （六）互联网门户网站泄露敏感信息
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条第五项和相关审慎经营规则
行政处罚决定			罚款420万元
作出处罚决定的机关名称			中国银行保险监督管理委员会
作出处罚决定的日期			2021年1月19日

3. 因客户信息保护机制不健全，中信银行被罚 450 万元

2021 年 3 月 17 日，中国银保监会发布的行政处罚信息显示，中信银行因客户信息保护体制机制不健全、客户信息收集环节管理不规范、违规存储、泄露客户敏感信息被处罚款 450 万元。

中国银行保险监督管理委员会行政处罚信息公开表
（银保监罚决字〔2021〕5号）

（中信银行股份有限公司）

行政处罚决定书文号			银保监罚决字〔2021〕5号
被处罚当事人	单位	名称	中信银行股份有限公司
		法定代表人姓名	李庆萍
主要违法违规事实（案由）			一、客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力 二、客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息 三、对客户敏感信息管理不善，致其流出至互联网；违规存储客户敏感信息 四、系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条和相关审慎经营规则 《中华人民共和国商业银行法》第七十三条
行政处罚决定			罚款450万元
作出处罚决定的机关名称			中国银行保险监督管理委员会
作出处罚决定的日期			2021年3月17日

4. 因信息安全违规，建行员工的直接责任人被罚禁止从业

2021 年 5 月，建设银行因员工违规查询、泄露客户信息以及未按规定报送涉刑案件（风险）信息，被罚 30 万，员工的直接责任人被罚禁止从事银行业工作 5 年。

黑龙江银保监局行政处罚信息公开表（黑银保监罚决字〔2020〕38号）

（中国建设银行股份有限公司哈尔滨河松支行）

行政处罚决定书文号			黑银保监罚决字〔2020〕38号
被处罚当事人姓名或名称	个人姓名		
	单位	名称	中国建设银行股份有限公司哈尔滨河松支行
		法定代表人（主要负责人）姓名	谭鸿燕
主要违法违规事实（案由）			前台业务管理不到位、员工行为排查不到位导致发生案件
行政处罚依据			《中华人民共和国银行业监督管理法》第四十六条
行政处罚决定			罚款30万元
作出处罚决定的机关名称			黑龙江银保监局
作出处罚决定的日期			2020年5月20日

黑龙江银保监局行政处罚信息公开表（黑银保监罚决字〔2020〕39号）

（魏阳光）

行政处罚决定书文号			黑银保监罚决字〔2020〕39号
被处罚当事人姓名或名称	个人姓名		魏阳光
	单位	名称	
		法定代表人（主要负责人）姓名	
主要违法违规事实（案由）			对建行哈尔滨河松支行前台业务管理不到位、员工行为排查不到位负管理责任
行政处罚依据			《中华人民共和国银行业监督管理法》第四十八条
行政处罚决定			禁止从事银行业工作5年
作出处罚决定的机关名称			黑龙江银保监局
作出处罚决定的日期			2020年5月20日

5. 因个人贷款业务管理漏洞，平安银行被罚 772 万

2020 年 7 月 11 日，京银保监罚决字〔2020〕21 号罚单显示，平安银行北京分行因存在采取不正当手段发放贷款，个人贷款业务内控管理存在多项缺陷，以表外资金掩盖表内承兑汇票垫款等 6 项违法违规行为，被监管处以 772.22 万元处罚，当事员工刘静被禁止 3 年内从事银行业工作。

北京银保监局行政处罚信息公开表

（北京银行城市副中心分行）

行政处罚决定书文号			京银保监罚决字〔2020〕24号
被处罚当事人	个人姓名		——
	单位	名称	北京银行城市副中心分行
		法定代表人（主要负责人）姓名	丁慈秀
主要违法违规事实（案由）			员工行为管理不到位。
行政处罚依据			《中华人民共和国银行业监督管理法》第二十一条、第四十六条。
行政处罚决定			责令北京银行城市副中心分行改正，并给予40万元罚款的行政处罚。
作出处罚决定的机关名称			北京银保监局
作出处罚决定的日期			2020年7月11日

6. 因侵犯公民个人信息，建设银行一支行行长被禁业五年

2021 年 10 月 22 日，银保监会网站公布一则行政处罚决定书公告送达书透露，沈静冲时任中国建设银行余姚城建支行行长，侵犯公民个人信息案件的作案当事人，对侵犯公民个人信息案件负有直接责任。

宁波银保监局表示，上述事实，有浙江省余姚市人民法院刑事判决书、中国建设银行宁波市分行案件信息确认报告、宁波银保监局案件调查事实确认书、行政处罚案件调查笔录等证据证明。

该公告显示，作为侵犯公民个人信息案件当事人，上述行为已触犯《中华人民共和国刑法》第二百五十三条的规定，违反了《银行业金融机构从业人员职业操守指引》（银监发〔2011〕6 号）第五条、第七条的规定，属于严重违反审慎经营规则的行为。

根据《中华人民共和国银行业监督管理法》第四十八条第（三）项规定，宁波银保监局决定对沈静冲予以禁止从事银行业工作五年的行政处罚。

行政处罚决定书公告送达

沈静冲：

我局 2021 年 9 月 2 日向你作出《行政处罚决定书》（甬银保监罚决字〔2021〕64 号），因采取其他送达方式无法送达，根据《中华人民共和国行政处罚法》第六十一条、《中华人民共和国民事诉讼法》第九十二条的规定，现向你公告送达。自公告之日起，经过六十日即视为送达。《行政处罚决定书》（甬银保监罚决字〔2021〕64 号）主要内容如下：

你时任中国建设银行余姚城建支行行长，是侵犯公民个人信息案件的作案当事人，对侵犯公民个人信息案件负有直接责任。

上述事实，有浙江省余姚市人民法院刑事判决书、中国建设银行宁波市分行案件信息确认报告、宁波银保监局案件调查事实确认书、行政处罚案件调查笔录等证据证明。

综上，我局决定作出如下行政处罚：

你作为侵犯公民个人信息案件当事人，上述行为已触犯《中华人民共和国刑法》第二百五十三条的规定，违反了《银行业金融机构从业人员职业操守指引》（银监发〔2011〕6 号）第五条、第七条的规定，属于严重违反审慎经营规则的行为。根据《中华人民共和国银行业监督管理法》第四十八条第（三）项规定，我局决定对你予以禁止从事银行业工作五年的行政处罚。

如不服本行政处罚决定，可以在收到本处罚决定书之日起六十日内向中国银行保险监

督管理委员会申请行政复议，也可以在收到本处罚决定书之日起六个月内向有管辖权的人民法院提起诉讼。复议、诉讼期间本决定不停止执行。

宁波银保监局

2021 年 10 月 22 日

附录：银行业金融机构行政处罚决定书统计表

序号	处罚时间	处罚文号	处罚对象	处罚原因	处罚金额	负责人处罚
1	2020/1/21	西银罚字〔2020〕第 7 号	交通银行股份有限公司陕西省分行	个人征信系统管理用户和查询用户兼职	1 万元	/
2	2020/1/21	西银罚字〔2020〕第 8、9 号	兴业银行股份有限公司西安分行	未及时停用已离岗工作人员用户	37.5 万元	1 万元
3	2020/1/21	西银罚字〔2020〕第 3-6 号	浙商银行股份有限公司西安分行	未及时停用已离岗离职工作人员用户	91.5 万元	合计 4.5 万元
4	2020/2/10	银罚字〔2020〕1-13 号	民生银行总行	未按规定履行客户身份识别义务、未按规定保存客户身份资料和交易记录、未按规定报送大额交易报告和可疑交易报告、与身份不明的客户进行交易	2360 万元	共 45 万元
5	2020/2/10	银罚字〔2020〕14-22 号	光大银行总行	未按规定履行客户身份识别义务、未按规定保存客户身份资料和交易记录、未按规定报送大额交易报告和可疑交易报告、与身份不明的客户进行交易	1820 万元	共 23.5 万元
6	2020/2/20	京银保监罚决字〔2020〕10 号	中信银行总行	共 19 项违法违规事实，多涉及贷款违规或房地产业务	2020 万元	
7	2020/2/20	赣银保监罚决字〔2020〕2 号	江西农信社联合社	对全省农村商业银行非现场监管信息系统报表数据管理不到位	50 万元	/

8	2020/3/5	成银罚字〔2020〕1～4号	中国进出口银行四川省分行	未按照规定报送大额交易报告或者可疑交易报告	60万元	合计4万元
9	2020/3/17	渝银处罚公示〔2020〕5号	重庆富民银行股份有限公司	虚报、瞒报金融统计资料；超过期限或未向中国人民银行报送账户开立、变更、撤销等资料；未按规定进行条码支付业务管理；未按照《征信业管理条例》的规定处理异议；未按规定履行客户身份识别义务；未按规定报送可疑交易报告；侵害消费者个人信息依法得到保护的权利	184.5万元	共8.5万元
10	2020/3/24	(南银)罚字〔2020〕第11号	杭州银行南京分行	超期或未报送账户开立、撤销等资料；明知是单位资金允许以自然人名称开立账户存储；未按规定履行客户身份识别义务；违规查询和使用客户个人信息	42万元	2.8万元
11	2020/4/1	渝银罚字〔2020〕16号	中国邮政储蓄银行股份有限公司重庆分行	未经同意查询个人信息；未准确、完整、及时报送个人信用信息	33万元	2万元
12	2020/4/3	深人银罚[2020]3号	深圳瑞银信信息技术有限公司	超出核准业务范围、未按规定建立有关制度办法或风险管理措施、未按规定履行客户身份识别义务、与身份不明客户进行交易、未按规定报送可疑交易报告	6124万元	共35.5万元
13	2020/4/3	南银罚字〔2020〕1号	南昌农村商业银行股份有限公司	违反反洗钱管理规定，未按规定履行客户身份识别义务，未按规定报送可疑交易报告，与身份不明的客户进	184万元	共29.8万元

				行交易或为客户开立匿名、假名账户违反支付结算管理规定，存在账户开立不合规问题 违反征信管理规定，未经授权查询个人或者企业的信贷信息，未按规定处理征信异议，超范围查询个人信用报告		
14	2020/4/10	鹤银罚字〔2020〕1号	中原银行股份有限公司鹤壁分行	未经同意查询个人信息或者企业的信贷信息；	18.4万元	共计 1.4万元
15	2020/4/14	长银罚字〔2020〕12号	华夏银行长春分行	越权查询个人信用数据库、个人信用报告管理不符合安全管理要求、未按规定创建异议处理用户、未按规定创建管理员用户、未按规定及时停用用户	21万元	/
16	2020/4/14	长银罚字〔2020〕8、9号	交通银行吉林省分行	未按照规定处理征信异议	/	共 2 万元
17	2020/4/14	长银罚字〔2020〕10号	交通银行长春红旗街支行	未经同意查询个人信息	/	1万元
18	2020/4/14	长银罚字〔2020〕3号	招商证券长春人民大街证券营业部	未按照规定履行客户身份识别义务	22万元	各 1.3万元
19	2020/4/14	长银罚字〔2020〕4-6号	中华联合财险吉林分公司	未按照规定履行客户身份识别义务	23.3万元	各 1.5万元
20	2020/4/16	邢银保监罚决字〔2019〕22号	长城人寿邢台中心支公司	客户信息真实性管理不规范、违反相关保险经营规则	4万元	各 1 万元

21	2020/4/22	晋中罚字〔2020〕2号	建设银行晋中分行	未按规定履行客户身份识别初次义务	8.5 万元	0.5 万元
22	2020/4/23	舟银保监罚决字〔2020〕6号	浙江岱山农商银行	违规泄露客户信息	30 万元	禁业三年
23	2020/4/27	大银保监罚决字〔2020〕20号	新华人寿保险股份有限公司大连分公司	欺骗投保人、银保业务数据不真实	32 万元	/
24	2020/4/30	郑银罚字〔2020〕15号	广发银行股份有限公司郑州分行	未按照规定处理征信异议	117.6 万元	1 万元
25	2020/5/1	银保监消保发〔2020〕1号	中国人保寿险、农行、邮储银行	中国人保寿险的部分客户信息数据不真实，存在核心业务系统投保人联系电话与客户回访系统最终回访电话不一致、登记的投保人联系电话非本人电话等问题；部分涉及可回溯管理的业务虚假；中国人保寿险报送的2017年个人医疗理赔数据不真实，存在案件数据遗漏、字段提取不符合相关通知中的要求等问题	618 万元	338 万元
26	2020/5/11	南宁银罚〔2020〕10-14号	中国建设银行股份有限公司广西壮族自治区分行	虚报涉农贷款专项统计数据；收纳的部分预算收入未及时划缴国库；未按照规定开展客户身份持续识别；未按照规定履行客户身份资料保存义务	58 万元	1/1/2.5 万元
27	2020/5/11	津银保监罚决字〔2020〕82-83号	中国邮政储蓄银行股份有限	未按照规定履行客户身份识别义务，未按照规定保存客户身份资料和交易记录	50 万元	3.5 万元

			公司广西壮族自治区分行			
28	2020/6/18	银管罚〔2020〕13号	厦门国际银行股份有限公司北京分行	超期向人民银行报备银行结算账户开立资料；未按规定履行客户身份识别义务；违反征信信息查询规定；未按规定立即停用调离工作人员的个人征信系统查询用户	347.5万元	15人合计罚款72万元
29	2020/6/24	银管罚〔2020〕12号	北京新浪支付科技有限公司	未落实特约商户管理责任；支付交易信息未落实真实、完整、可追溯要求；为不符合规定的商户开通代收业务；未按规定与外包服务机构开展业务合作；违规开立与使用支付账户；未按规定管理客户备付金；未按规定公开披露有关事项；未按规定办理相关变更事项；未按规定建立相关制度办法	1718.44万元	35万元
30	2020/7/3	甬银处罚字〔2020〕8号	中信银行宁波分行	1.未准确报送个人信用信息；2.违规为存款人多头开立银行结算账户；3.超过期限或未向中国人民银行报送账户开立、变更、撤销等资料；4.违反票据法规定进行承兑、贴现；5.未按照规定履行客户身份识别义务；6.未按照规定保存客户身份资料和交易记录；7.未按照规定报送大额交易报告和可疑交易报告。	129万元	3万元
31	2020/7/16	粤银保监罚决字〔2020〕28号	广发银行信用卡中心	未向持卡人披露信用卡总授信额度信息、未审慎设定信用卡预借现金业务授信额	180万元	/

				度、未有效履行信用卡客户身份识别义务		
32	2020/7/17	上海银罚字〔2020〕12-17、19号	兴业银行上海分行	未执行金融统计制度，错报统计数据；未按规定报备人民币结算账户开户资料；国库经收业务未使用规定科目核算；未按照规定履行客户身份识别义务；发布引人误解的营销宣传信息。	123.5 万元	合计 10.5 万元
33	2020/8/14	沪银保监银罚决字〔2020〕14 号	上海银行	关联交易管理严重不审慎；未按规定保存重要信贷档案，导致分类信息不准确、不完整；未按规定报送统计报表等 23 项违法	1625 万元	/
34	2020/8/17	沈银罚字〔2020〕5-10 号	建设银行辽宁分行	1.个别预算收入业务未使用“待结算财政款项”科目收纳和核算； 2.未按规定履行客户身份识别义务； 3.未按规定保存客户身份资料和交易记录； 4.与身份不明的客户进行交易。	169.5 万元	11.5 万元
35	2020/8/27	深银罚〔2020〕12-14 号	浙商银行深圳分行	1.超过期限或未向中国人民银行报送账户开立、变更、撤销等资料； 2.未有效落实防范对外误付假币措施； 3.未及时报送个人信用信息； 4.未按照规定履行客户身份识别义务"	98.1 万元	合计 6.75 万元
36	2020/8/27	深人银罚〔2020〕20 号	建设银行深圳市分	未按照规定履行客户身份识别义务；	204 万元	合计 19.1 万元

			行	未按照规定保存客户身份资料和交易记录； 未按照规定报送可疑交易报告。		
37	2020/9/4	福银罚字〔2020〕30、33、35号	兴业银行福州分行	1.为无证机构提供转接清算服务，且未落实交易信息真实性、完整性、可追溯性及支付全流程中的一致性的规定；2.为支付机构超范围（超业务、超地域）经营提供支付服务，且未落实交易信息真实性、完整性、可追溯性及支付全流程中的一致性；3.违规连通上、下游支付机构，提供转接清算服务，且未落实交易信息真实性、完整性、可追溯性及支付全流程中的一致性；4.违反银行卡收单外包管理规定；5.未按规定履行客户身份识别义务。	1382.44万元	合计14万元
38	2020/9/4	福银罚字〔2020〕29、32、34号	福建海峡银行	1.违反银行卡收单外包管理规定 2.未按规定履行客户身份识别义务	93万元	合计7.5万元
39	2020/9/7	福银罚字〔2020〕41-46号	招商银行福州分行	1.未按规定履行客户身份识别义务；2.未按规定保存客户交易记录；3.存在引人误解的营销宣传内容；4.个体工商户经营性贷款统计错误；5.为新增特约商户通过不同法人机构间直连的支付通道处理条码支付业务；6.收纳的税款延迟划缴国库；7.将预算单位零余额账户资金转入内部其他账户；8.现金自助存取款设备对外支付	303.5万元	合计24.8万元

				残损人民币。		
40	2020/9/7	福银罚字〔2020〕37-40 号	中信银行福州分行	未按规定履行客户身份识别义务	140 万元	合计 3 万元
41	2020/9/11	福银罚字〔2020〕49-51、53-57 号	建设银行福建省分行	1.未按规定履行客户身份识别义务；2.未按规定报送可疑交易报告；3.存在引人误解的营销宣传内容；4.个体工商户经营性贷款统计错误；5.未按规定开展账户报备；6.违规开展代付业务；7,将预算单位零余额账户资金转入内部其他账户。	314 万元	合计 18.2 万元
42	2020/9/11	福银罚字〔2020〕47、48、52、58 号	海峡金桥财产保险股份有限公司	1.未按规定履行客户身份识别义务；2.未按规定保存客户交易记录	80 万元	合计 11 万元
43	2020/9/14	上海银罚字〔2020〕29 号	广发银行上海分行	1.未执行金融统计制度错报统计数据； 2.未按规定履行反洗钱义务； 3.发布引人误解的营销宣传信息； 4.未经审批查询个人金融信息。	174 万元	3.5 万元
44	2020/9/25	银管罚 27-29 号	盛京银行股份有限公司北京分行	1.开立单位银行结算账户未向人民币银行结算账户管理系统进行报备； 2.撤销单位银行结算账户超过期限上报或报备； 3.开立个人银行结算账户超过期限向人民币银行结算账户管理系统备案； 4.未经授权查询企业信用报告(含信贷信息）；	299.5 万元	两位反洗钱主管行长共计罚款 9.2 万元：营业部综合员罚款 1 万元

				5.未及时停用离职人员的个人征信系统查询用户； 6.未按照规定履行客户身份识别义务； 7.未按照规定开展客户身份资料及交易记录保存工作		
45	2020/9/28	银管罚〔2020〕29号	北京农商银行	1.为身份不明的客户提供服务或与其进行交易； 2.未按照规定履行客户身份识别义务； 3.未按照规定报送大额交易或可疑交易报告； 4.未按照规定履行客户身份资料及交易记录保存义务	1948万元	共计16万元
46	2020/10/19	德银罚字〔2020〕1号	中国建设银行股份有限公司德阳分行	侵害消费者个人信息依法得到保护的权利	1406万元	/
47	2020/10/20	宁银罚〔2020〕2号	中国银行石嘴山市分行	侵害消费者个人信息依法得到保护的权利	411万元	/
48	2020/10/20	东银罚字〔2020〕1号	中国建设银行股份有限公司东营分行	侵害消费者个人信息依法得到保护的权利	514万元	/
49	2020/10/20	长银罚字〔2020〕第8号	中国建设银行股份有限公司娄底市分行	侵害消费者个人信息依法得到保护的权利	533万元	/
50	2020/10/20	吉市银罚字〔2020〕2-6号	中国农业银行股份有限公司吉林市江	1.侵害消费者个人信息依法得到保护的权利； 2.违反反洗钱管理规定，泄	警告，并处1223万元罚款	合计8.25万元（该支行营业室员

			北支行	露客户信息		工罚款 3 万元，该支行行长、副行长、营业室业务主管共罚款 5.25 万元)
51	2020/10/27	上海银罚字〔2020〕30-31 号	交通银行股份有限公司上海市分行	作为备付金存管银行或备付金合作银行，未履行监督职责，未按规定办理新开立个人银行结算账户备案	警告，罚款 56.5 万	/
52	2020/10/29	银石罚字〔2020〕1 号	中国银行河北省分行	1.未按照规定履行户身份识别义务； 2.未按照规定报送大额交易报告或者可疑交易报告	310 万元	9.5 万元
53	2020/10/29	银石罚字〔2020〕2 号	中国银行石家庄管理部	1.未按照规定履行户身份识别义务； 2.未按照规定报送大额交易报告或者可疑交易报告	290 万元	7 万元
54	2020/10/29	银石罚字〔2020〕3 号	中国银行辛集分行	1.未按照规定履行户身份识别义务； 2.未按照规定报送大额交易报告或者可疑交易报告	180 万元	7 万元
55	2020/10/29	银石罚字〔2020〕4 号	中国银行保定分行	1.未按照规定履行户身份识别义务； 2.未按照规定保存客户身份资料和交易记录	70 万元	3.5 万元
56	2020/10/29	银石罚字〔2020〕5 号	中国银行定州分行	未按照规定履行户身份识别义务；	60 万元	3.5 万元
57	2020/10/29	银石罚字〔2020〕6 号	中国银行邢台分行	1.未按照规定履行户身份识别义务；	130 万元	7 万元

				2.未按照规定保存客户身份资料和交易记录		
58	2020/11/16	西银罚字〔2020〕18-21号	广发银行股份有限公司西安分行	1.个人征信查询用户调离未及时禁用、个人征信用户新增未及时向当地人民银行进行备案； 2.超过期限向人民银行报送账户开立资料； 3.未按规定履行客户身份识别义务； 4.未按规定报送可疑交易报告	228.5万元	共计14.2万元
59	2021/1/7	晋市银罚字〔2021〕第2号	晋城银行股份有限公司	违反《征信业管理条例》第二十八条第二款之规定，未取得信息主体书面同意查询信用报告。违反《个人信用信息基础数据库管理暂行办法》第二十九条第二款之规定，未按规定向人民银行备案用户变更情况。	单位处以罚款52万元	对1名直接负责的主管人员处以罚款3万元，对1名直接责任人员处以罚款2万元
60	2021/1/8	兰银罚字〔2021〕第1号	甘肃榆中农村合作银行	1.虚报、瞒报金融统计资料。 2.超过期限或未向中国人民银行报送账户开立、变更、撤销等资料。 3.对外付出现金中夹杂不宜流通人民币；现金从业人员业务知识不足，判断和挑剔假币的专业能力不足；部分营业网点现金机具鉴别能力不足。 4.零余额账户有贷方余额。 5.征信内控制度未备案；用	警告、69.9万元	

				户未报备或报备不及时；查询信用报告未取得客户授权。 6.未按规定履行客户身份识别义务。		
61	2021/1/12	福银罚字〔2021〕61号	中国人民银行福州中心支行	1.未按规定履行客户身份识别义务；未按规定保存客户身份资料； 2.未按规定报送可疑交易报告； 3.与身份不明的客户进行交易； 4.条码支付业务风控制度不健全； 5.未按规定办理董事、监事和高级管理人员变更； 6.未按规定存放客户备付金； 7.未按规定真实、完整地发送交易信息，且未落实交易信息的完整性、真实性、可追溯性及支付全流程中的一致性的规定； 8.为不符合条件的客户提供T+0资金结算服务； 9.未按规定开展收单交易风险监测； 10.存储银行卡敏感信息； 11.未备案先展业。	警告，并没收违法所得261.02万元，处6710.02万元罚款，合计罚没6971.04万元	
62	2021/1/27	银管罚〔2021〕3号	新韩银行（中国）有限公司	未经同意查询个人征信信息	57万元	
63	2021/1/29	银保监罚决字	中国农业	1.发生重要信息系统突发事	罚款420	

		〔2021〕1号	银行	件未报告； 2.制卡数据违规明文留存； 3.生产网络、分行无线互联网络保护不当； 4.数据安全管理较粗放，存在数据泄露风险； 5.网络信息系统存在较多漏洞； 6.互联网门户网站泄露敏感信息。	万元	
64	2021/2/3	沈银罚字〔2021〕5-8号	中国银行股份有限公司辽宁省分行	1.因未按规定收集、使用消费者个人金融信息； 2.营销活动中违规进行引人误解宣传； 3.备案类单位银行结算账户销户超期向人民银行备案； 4.代理国库存在违规问题； 5.未按规定履行客户身份识别义务	警告并处罚 114.7万元	/
65	2021/2/19	渝银罚〔2021〕4号	重庆市钱宝科技服务有限公司	1.未落实加强特约商户管理的相关规定； 2.未按规定进行收单银行结算账户管理； 3.未按规定办理相关备案手续； 4.未按规定公开披露相关事项； 5.未确保交易信息在支付全流程中的一致性； 6.未按规定办理相关变更事项； 7.未按规定履行客户身份识别义务；	警告并罚款 868 万元	共计 48.5 万

				8.未按规定保存客户身份资料； 9.未按规定报送可疑交易报告； 10.开立假名匿名账户。		
66	2021/3/1	长银罚字〔2021〕1号	湖南东安农村商业银行股份有限公司	1.未及时更新、非法使用个人金融信息； 2.金融统计错误； 3.开立单位结算账户未向人民银行备案以及开立企业类银行账户备案不及时； 4.未按照规定初次识别客户身份和重新识别客户身份； 5.对清分发现假币不收缴； 6.未按规定将假币解缴中国人民银行分支机构； 7.假币收缴凭证登记要素缺失； 8.“先清算后支付”，占压财政性资金； 9.未经同意查询个人信用报告； 10.对征信异议处理不规范。	69.5万元	共计2.8万元
67	2021/3/19	银保监罚决字〔2021〕5号	中信银行股份有限公司	1.客户信息保护体制机制不健全；柜面非密查询客户账户明细缺乏规范、统一的业务操作流程与必要的内部控制措施，乱象整治自查不力。 2.客户信息收集环节管理不规范；客户数据访问控制管理不符合业务“必须知道”和“最小授权”原则；查询客户	450万元	/

				账户明细事由不真实；未经客户本人授权查询并向第三方提供其个人银行账户交易信息。 3.对客户敏感信息管理不善，致其流出至互联网；违规存储客户敏感信息。 4.系统权限管理存在漏洞，重要岗位及外包机构管理存在缺陷。		
68	2021/4/6	长银罚字〔2021〕6号	吉林亿联银行股份有限公司	1.涉及未准确、完整、及时报送个人信用信息； 2.未按规定处理异议； 3.未按规定报送大额交易报告或可疑交易报告； 4. 为客户开立匿名、假名账户	164.4 万元	共计 14.2 万元
69	2021/4/6	长银罚字〔2021〕14-17 号	渤海银行股份有限公司长春分行	1.未向中国人民银行报送账户开立资料； 2.未准确、完整、及时报送个人信用信息； 3.未按照规定处理异议； 4.未经同意查询个人信息； 5.未按规定履行客户身份识别义务。	58.6 万元	共计 4.4 万元
70	2021/4/7	津银罚字〔2021〕4号	平安银行股份有限公司天津分行	1.违规开展金融营销宣传行为； 2.违规收集与业务无关的第三人信息	45 万元	/
71	2021/4/13	西银罚字〔2021〕6-13 号	长安银行股份有限公司	违反支付结算、反洗钱、货币金银、国库、征信管理规定	420.8 万元	
72	2021/5/7	哈银罚字〔2021〕4-7 号	哈尔滨农村商业银行股份有	1、未按规定履行客户身份识别义务； 2、未按规定保存客户身份	违法行为 1 至 4：罚款 478	合计 9.2 万元

			限公司海城支行	资料和交易记录； 3.未按规定报送大额交易报告和可疑交易报告； 4、与身份不明的客户进行交易或者为客户立匿名账户、假名账户 5、虚报、瞒报金融统计资料； 6、未经同意查询个人信息。	万元；违法行为5：警告，并处罚款1万元；违法行为6：罚款6万元	
73	2021/5/17	渝银保监罚决字〔2021〕33号	重庆市沙坪坝融兴村镇银行有限责任公司	1.虚报、瞒报金融统计资料； 2.超过期限或未向中国人民银行报送账户开立、变更、撤销等资料； 3.提供个人不良信息，未履行不良告知义务； 4.异常交易排除理由不合理。	给予警告，并处46.5万元罚款	1万元
74	2021/5/21	包银罚字〔2021〕1、2号	鄂尔多斯银行股份有限公司包头分行	1. 未按照规定有效履行客户身份识别义务。 2. 虚报、瞒报金融统计资料。 3. 违反《个人信用信息基础数据库管理暂行办法》安全管理要求。 4. 将残缺、污损的人民币对外支付。 5. 超过期限或未向中国人民银行报送账户开立、变更、撤销等资料。	35.8万元罚款	/
75	2021/5/26	绵银罚字〔2021〕2-4号	四川江油华夏村镇银行股份有限公司	1. 虚报、瞒报金融统计资料； 2. 超过期限或未向中国人民银行报送账户开立、撤销	49.5万元罚款	/

				等资料； 3．未按规定收缴假币； 4．未按照与个人信息主体约定的用途使用个人信息； 5．未按照规定报送大额交易报告或者可疑交易报告。		
76	2021/7/6	合银罚字〔2021〕3-6号	中国银行股份有限公司安徽省分行	1．开立银行结算账户未核准或未按规定备案； 2．非个体工商户商户使用个人账户作为收单结算账户， 3．未按规定收缴假币； 4．发生假币误收行为； 5．未按规定履行客户身份识别义务； 6．未按规定报送可疑交易报告； 7．ETC预登记业务侵害消费者个人信息权利。	114.7万元罚款	/
77	2021/7/14	广州银罚字〔2021〕4-7号	广东南粤银行股份有限公司	超过期限向中国人民银行报送账户撤销资料；违反人民币现金收付与货币防伪反假管理规定；违反国库管理规定；违反征信管理规定。	172.2万元	共计6.2万元
78	2021/8/2	南银罚字〔2021〕1-3号	江西新建农村商业银行股份有限公司	1.提供虚假的金融统计数据； 2.未按规定向人民银行报送账户开立、变更、撤销等资料； 3.发现假币未收缴； 4.未按规定收缴假币； 5.违反信用信息采集、提供、查询及相关管理规定； 6.未按规定履行客户身份识别义务；	430.5万元	总计11.75万元

				7.未按规定报送大额交易报告或者可疑交易报告； 8.与身份不明的客户进行交易或者为客户开立匿名账户、假名账户。		
79	2021/8/5	福银罚字〔2021〕35-46号	福建福州农村商业银行	1.未按规定履行客户身份识别义务； 2.未按规定报送大额交易和可疑交易报告； 3.与身份不明的客户进行交易； 4.提供个人不良信息，未事先告知信息主体本人； 5.未经同意查询个人信息；网点发生误收假币行为； 6.清分中心未按规定收缴假币； 7.将预算收入转入“待结算财政款项”以外其他账户； 8.占压财政资金； 9.小微商户交易限额管理不到位； 10.对涉诈银行结算账户交易监测及管控不到位； 11.个人银行结算账户开户未备案及超期备案； 12.违规开立子账户； 13.存在虚假或引人误解的营销宣传	658万元	共计35.3万元
80	2021/8/6	乌银罚字〔2021〕2号	中国邮政储蓄银行股份有限公司新疆分行	1.违反反洗钱相关规定的行为 2.违反支付结算相关规定的行为 3.违反征信管理相关规定的	185万元	共计7.4万元

				行为		
81	2021/8/9	武银罚字〔2021〕11-15号	招商银行股份有限公司武汉分行	1.违反清算管理规定、违反人民币银 行结算账户管理相关规定 2.违反假币收缴鉴定管理相关规定、 违反人民币管理相关规定 3.违反代理国库业务相关规定 4.违反征信管理相关规定 5.未按规定履行客户身份识别义务、 与身份不明客户进行交易 6.金融产品宣传与实际不符	254.3万元	共计12万元
82	2021/8/13	银罚字〔2021〕23-24号	交通银行股份有限公司	违反信用信息采集、提供、查询及相关管理规定。	62万元	7万元
83	2021/8/13	银罚字〔2021〕25号	华夏银行股份有限公司	违反信用信息采集、提供、查询及相关管理规定。	486万元	/
84	2021/8/20	成银管罚字〔2021〕4-7号	四川成都蒲江民富村镇银行有限责任公司	违反信用信息采集、提供、查询及相关管理规定	98.5万元	共计1.6万元
85	2021/9/29	渝银保监罚决字〔2021〕30号	重庆富民银行股份有限公司	两会一层在互联网贷款管理流程中履职不到位；	850万元	负有直接责任人员被处以共计100万元罚款，并被警告

本选编仅属于内部研究交流资料，不应对外销售或公开传播

安证合规研究院
广东北源律师事务所 编