[网络与金融数据合规研讨会内容摘要]

2021 年 9 月 28 日，观韬中茂律师事务所召开网络与金融数据合规研讨会。此次会议由李洪江律师主持，共分为两个部分，第一部分由吴丹君律师、张振君律师、徐颖文律师展开网络数据安全领域相关主题分享，第二部分由首席风控合规官发起人陈能杰作为主持人，组织线下在场人员进行数据合规研讨交流，共同探讨数据合规领域的时下热点及前瞻性展望。共有数十名法律从业人员、企业高管人员、金融行业从业人员通过北京办公室现场以及线上方式进行参会交流，以下是会议内容部分摘要：

一、吴丹君律师——金融行业数据合规重点简述

吴丹君律师从以下三个方面针对金融行业数据合规重点进行了详细的介绍：

（一）网络安全与数据保护法律体系

为理解我国网络安全与数据保护法律体系，首先需厘清两对关系，一是数据和个人信息的概念辨析，二是数据安全与网络安全的联系。数据是指任何电子或其他方式对信息的记录，不仅包括电子数据，也包括纸质等其他方式记录的信息；个人信息则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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号

码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。数据与个人信息的关系紧密，个人信息为数据的一部分，而基于海量个人信息形成的统计数据、衍生数据还可能属于重要数据。因此，金融机构在数据治理中不能忽略个人信息的保护。其次，在数据安全与网络安全的关系上，《数据安全法》规定，利用互联网等信息网络开展数据处理活动，应在网络安全等级保护制度的基础上进行，因而网络安全是保障数据安全的前提。

我国《数据安全法》推动很多部门、行业组织、科研机构、企业等共同参与数据安全保护工作，从监管部门职责、数据类型、社会主体参与等多种角度，构建起一个多方参与的治理体系。然而，由于未建立统一的监管机构，我国的数据安全治理尚处于一个“九龙治水”的局面。

（二）金融数据的特殊合规风险

近些年，伴随金融场景服务的线上化、多样化，面对金融科技不断发展、法律法规逐渐完善、疫情冲击下的数字化转型的现状，金融数据的特殊风险逐渐凸显，主要集中在以下几点：a、金融数据敏感程度高； b、全流程金融数据安全管理制度体系尚未形成； c、金融数据营销利用、共享传输需求高；d、金融数据安全事件发生风险高；e、严重情况下可能导致刑事风险。

（三）全流程金融数据安全管理制度的建设

总体而言，面对金融数据的特殊合规风险，全流程金融数据安全管理制度亟需建设，主要可从以下几个方面开展：

一是建立数据分类分级管理制度，分类分级管理是数据安全管理制度构建的首要环节。但金融机构对某类金融数据级别的判断并非“一劳永逸”，因为金融数据的风险会随着所涉及的数据内容、数据规模、数据来源和业务特点等因素而处于动态变化的过程中，金融机构需实时关注数据风险变化，及时调整数据的安全级别并采取相应等级的安全措施。

二是完善金融数据安全保障措施，包括制度措施及技术措施。金融机构应在数据分类分级基础上，建立定期风险监测、风险评估以及安全应急制度，并在前述制度指引下参考《金融数据生命周期安全规范》《金融业数据能力建设指引》等文件采取相应技术措施。

三是加强金融数据处理人员管理，包括完善岗位设置、按照最小必要、职权

分离等原则，授予不同账户为完成各自承担任务所需的最小权限，明确数据权限申请和变更等审批流程。同时，还应依法按需设置重要数据管理部门或个人信息保护部门，与可接触重要数据或个人金融信息的员工签订保密协议，并定期开展员工培训。

四是加强第三方服务供应商管理，与第三方服务供应商的数据传输可能加大数据泄露的安全风险及数据滥用风险，建议通过签署协议、采取数据脱敏等技术措施进行预先防范。

最后是保障金融数据在跨境传输中的安全。结合《数据安全法》和《个人信息保护法》，可将我国金融数据出境分为“三步走”，第一步判断境外接收方性质，第二步判断境内提供者性质，第三步判断拟传输数据性质，最终拟定和执行数据出境方案。

二、张振君律师——App 数据合规/金融行业的合规问题

张振君律师从以下三个方面针对金融 App 数据合规问题进行了详细介绍：

（一）金融 App 数据合规的法律背景

金融App的数据合规要求一般会比普通App更高。一是就所处理的数据而言，金融数据例如银行账户信息等具有更高的敏感性和价值，这也增加了其受侵害风险；二是立法方面，目前我国相关立法出台较为密集，央行曾在 2019 年发布《移动金融客户端应用软件安全管理规范》，在今年 5 月生效的《常见类型移动互联网应用程序必要个人信息范围规定》也对网络支付、投资理财、手机银行等类型的金融 App 的必要个人信息处理范围作出指引；三是执法方面，工信部、网信办等部门目前执法活动活跃，对 App 的监管力度较强。此外，针对金融机构的数据合规监管，双罚制逐渐成为常态。

（二）App 数据合规工作开展

面对目前的立法和监管态势，金融 App 数据合规工作的开展可从以下四个方面进行，一是加强金融机构的数据保护制度保障和技术支持；二是梳理业务功能，将 App 功能分为基本业务功能和拓展业务功能。根据实现某项业务功能所需的必要数据来设计相应数据处理方案，如需处理敏感个人信息的，应提前设计单独同意机制。；三完善 App 的页面设计和文本设计，包括隐私政策在 App 的位置，首

次运行时是否有弹窗提示、四次点击能否打开隐私政策，是否提供简体中文版本、文字是否过小过密，是否关注老年人等特别群体等等；四是建立风险监测管理机制，包括对 App 潜在安全风险的监测，亦包括对法律要求变化的关注。同时，根据《中国人民银行关于发布金融行业标准加强移动金融客户端应用软件安全管理的通知》，金融 App 应每年至少开展一次外部评估，形成报告存档备查。

（三）金融 App 数据合规自查

金融 App 的数据合规自查可分为以下四个合规模块开展：

一为运营资质自查，除从事该项金融业务需要的相关资质外，是否具备增值电信经营许可证或者 ICP 备案等其他资质。

二为金融机构的安全防护能力自查，金融机构应加强客户端软件设计、开发、发布、维护等环节的安全管理，构建覆盖数据全生命周期的管理机制，采取有效措施防范、应对网络攻击，保障相关系统平稳安全运行。

三为金融 App 的身份认证安全能力自查，主要考察金融机构是否能在准确识别用户身份的同时保障认证信息的安全。

第四，则为个人金融信息保护能力自查。金融机构是否在数据收集、使用、存储、加工、传输、对外提供等各个环节落实个人信息保护的相关要求，包括隐私政策、用户协议的设计和 App 的页面设计，接入 SDK 等第三方产品或服务时采取的安全保障措施，还有内部个人信息保护制度的制定，岗位和人员的设置及技术措施的采取是否满足个人金融信息的保护要求。最后，张振君律师针对个人金融信息保护能力合规模块，结合合规自查清单进行详细解读，供与会人员参考。

三、徐颖文律师—金融机构如何构建防范侵犯公民个人信息罪风险合规体系

徐颖文律师从以下两个方面针对金融机构数据合规的刑事风险进行了详细的报告：

（一）《刑法》中关于个人金融信息的分类

刑法第二百五十三条规定：“【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。”

《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第五条规定：非法获取、出售或者提供公民个人信息，具有下列情形之一的，应当认定为刑法第二百五十三条之一规定的“情节严重”：（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；（二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；（三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；（四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；（五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；（六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；（七）违法所得五千元以上的；（八）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，数量或者数额达到第三项至第七项规定标准一半以上的；（九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的；（十）其他情节严重的情形。实施前款规定的行为，具有下列情形之一的，应当认定为刑法第二百五十三条之一第一款规定的“情节特别严重”：（一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；（二）造成重大经济损失或者恶劣社会影响的；（三）数量或者数额达到前款第三项至第八项规定标准十倍以上的；（四）其他情节特别严重的情形。

根据以上条款的规定，可以看出，我国对于信息的刑法保护分为三个层次：

一类：行踪轨迹、通信内容、征信信息、财产信息。（50 条入罪，银行工作人员在履行职责中非法获取泄漏 25 条入罪）

二类：住宿信息、通信信息、健康生理信息、交易信息（如交易指令、交易流水）等其他可能影响人身、财产安全的信息。（500 条入罪，银行工作人员在履行职责中非法获取泄漏 250 条入罪）

三类：账户开立时间、开户机构等其他信息 。（5000 条入罪，银行工作人员在履行职责中非法获取泄漏 2500 条入罪）

此外，《个人金融信息保护技术规范》根据信息泄漏造成的后果进行个人金融信息敏感程度将信息分为以下三类：C3 信息包括用户鉴别信息：银行卡密码、支付密码、生物识别信息（包括人脸信息）；C2 信息包括支付账号及其等效信息；C1 包括账户开立时间、开户机构、支付标记信息等。其中两种低敏感的信息可能关联后成为高敏感信息。对于信息的分类保护需要加强关注。

（二）当前司法环境下的个人信息保护的趋势

目前相关部门正在某些地区开展合规不起诉制度的试点，这对于相关企业来说是一个利好消息，其中启动合规不起诉的考量因素包括：合规基础、社会危害性、科研、知识产权及上市背景、纳税就业情况、人员构成等等。

声明

本文件仅供参考，不能作为正式法律意见和建议。如果您有特定的法律问题或者需要法律意见，请与我们联系。

观韬中茂律师事务所