**新冠疫情下金融科技公司的金融安全义务**

新型冠状病毒感染的肺炎疫情发生后，呈现扩散趋势，为加强疫情防控，减少人员聚集，阻断疫情传播，国务院发布《国务院办公厅关于延长2020年春节假期的通知》。随后，各地区也纷纷出台相关政策，要求延期复工或在家办公。不少企业也响应政府政策，纷纷启动远程办公机制。

在此特殊情形下，不少线下业务减少，转而通过线上办理。各线上系统需及时响应，通过强化交易检测、有序承载增长的业务量，最终得以保障金融安全。

近期，中国人民银行和证监会发布一系列通知，提出了一系列支持疫情防控的措施，鼓励线上交易，要求加大电子支付服务保障力度。对此，各金融科技公司在提供常规服务外，更要加强疫情防控期间的业务承载过程中的风险防控，加强对交易安全和数据安全的保障。

**一、金融科技分类现状及主要监管规定**

（一）金融科技公司分类

我们根据目前市场上金融科技公司的原生背景，将其分为两类：一类为脱胎于商业银行的银行系金融科技公司，一类为来源于互联网科技公司的互联网系金融科技公司。

银行系金融科技公司具有天然的品牌优势和线下优势，依托银行领域的业务管理经验，风控水平高，稳定性强。服务对象主要以集团、同业为主，以中小企业为辅。

互联网系金融科技公司背靠着雄厚的技术实力，具有丰富的线上资源，服务对象面向大量企业客户和个体用户。

巴塞尔银行监管委员会将金融科技业务模式分为以下四类：支付结算、存贷款与资本筹集、投资管理、市场设施。基于此定位，金融科技产品和服务对安全的要求注定与传统的信息安全不同。传统的信息安全侧重的高保密性、完整性和可用性，而金融科技在满足传统的信息安全需求的同时，更侧重于交易安全和数据安全。

（二）监管部门及主要相关规定

目前，金融科技公司主要受网信办、工信部、公安部、央行、银保监会、证监会等多部门监管。

根据《中华人民共和国网络安全法》第二十一至第五十条之规定，网络运营者在**网络运行安全方面和网络信息安全方**面应尽保护义务。比如：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、篡改等；对其收集的用户信息**严格保密**，不得泄露、篡改、毁损其收集的个人信息；**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等。

根据《非银行支付机构网络支付业务管理办法》之相关规定，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**。

银保监会发布《银行业金融机构数据治理指引》，旨在**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。

中央网信办、工业和信息化部、公安部、市场监管总局联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，要求App运营者严格规范收集使用个人信息行为，**加强对个人信息保护**。

此外，在数据安全和网络安全方面的管理办法，如《数据安全管理办法(征求意见稿)》、《网络安全审查办法（征求意见稿）》，也已处于公开征求意见的阶段，相信不久也会逐步出台。

由此可见，保障交易安全、加强数据管理、保障信息安全，是金融科技的发展趋势，而切实履行金融安全义务也成为了对金融科技公司的基本要求。

**二、相关案例**

《中华人民共和国网络安全法》自2017年06月01日起正式实施至今，两年半的时间里，我们在中国裁判文书网，仅以“网络安全法”为关键词检索相关案例，就检索到134例案件。其中2016年1例，2017年6例，2018年53例，2019年74例。可以明显看到，涉嫌网络安全的的案件呈现上升趋势，这也侧面反映了网络安全方面还是存在很多问题，同时，各方对于网络安全的重视程度也在不断提升。

因篇幅有限，仅以数据安全案件举例说明之。在深圳市中级人民法院审理的周裕婵、广东快客电子商务有限公司网络侵权责任纠纷（案号：（2019）粤03民终3954号）中，法院认为网络运营者在收集、处理众多消费者个人信息过程中应履行依法收集、合理使用、安全防护、禁止或限制披露等义务。对于其提供服务所采集的用户信息数据，具有严格保密的法律义务。最终认定在该消费者信息泄露的案件中，网络运营者疏于防范，具有过错，应承担侵权责任。

因此，保护数据安全、保障交易安全是金融安全义务应有之意，这是所有金融科技运营主体的社会责任，也是所有金融科技运营主体应尽的法律义务。

**三、新冠疫情发生后，监管机构发布鼓励线上展业的通知**

2020年1月26日，银保监会发布《关于加强银行业保险业金融服务配合做好新型冠状病毒感染的肺炎疫情防控工作的通知》（银保监办发〔2020〕10号），通知要求各银行保险机构要根据疫情防控工作需要，合理安排营业网点及时间，保障基本金融服务和关键基础设施稳定运行。对受疫情影响临时停业或调整营业时间的网点，要主动做好解释说明，提供替代解决方案。**鼓励积极运用技术手段，在全国范围特别是疫情较为严重的地区，加强线上业务服务，提升服务便捷性和可得性。**

2020年1月27日，证监会发布《关于做好新型冠状病毒感染的肺炎疫情防控工作的通知》（证监办发〔2020〕9号），通知要求改进服务方式。从防止疫情扩散和保护投资者健康出发，耐心细致做好解释说明，**引导投资者采取非现场方式进行交易活动，并为非现场交易提供有效的技术保障和相关服务**。

2020年1月31日，中国人民银行发布《中国人民银行 财政部 银保监会 证监会 外汇局关于进一步强化金融支持防控新型冠状病毒感染肺炎疫情的通知》（银发〔2020〕29号），**要求加大电子支付服务保障力度**。支持银行业金融机构、非银行支付机构在疫情防控期间，**采用远程视频、电话等方式**办理商户准入审核和日常巡检，通过交易监测强化风险防控。鼓励清算机构、银行业金融机构和非银行支付机构对特定领域或区域特约商户实行支付服务手续费优惠。银行业金融机构、非银行支付机构要**强化电子渠道服务保障，灵活调整相关业务限额，引导客户通过电子商业汇票系统、个人网上银行、企业网上银行、手机银行、支付服务APP等电子化渠道在线办理支付结算业务**。

**四、疫情下金融科技公司履行金融安全义务的建议**

纵观全球金融行业，金融科技领域发生的安全事故屡见不鲜。如2017年9月，美国征信机构Equifax被曝遭遇黑客攻击，大量客户信息被窃取，约有1.42亿美国用户的个人重要信息面临泄漏; 2018年5月，加拿大两家银行遭到攻击，9万名客户信息遭泄露；2018年11月，美国汇丰银行通知客户10月4日至10月14日期间发生了数据泄露，约1%美国客户的个人信息被泄露。

科技行业也相继暴露出员工监守自盗、机房失火、P2P行业暴雷、数据泄露等问题，仅2019年国内，就出现了MongoDB数据库无人看管导致超2亿中国求职者简历疑泄露、京东金融APP被曝获取用户隐私、抖音千万级账号遭撞库攻击、阿里云宕机致大波互联网公司网站瘫痪、湖北首例入侵物联网系统案造成十万设备受损等这种重大事故。

交易安全和数据安全历来是金融科技领域的工作重点，而值此疫情影响的特殊期间，线上需求越是急迫，越是要保障交易安全和数据安全，避免其暴露于薄弱环节，引发金融安全事故。因此，我们建议：

（一）疫情期间，金融科技公司应提高各类业务的审核效率，简化流程，但涉及用户个人信息的流程不宜简化，仍应严格审核。

根据监管部门的通知，在疫情期间，金融科技公司应完善受疫情影响的社会民生领域的金融服务；通过技术手段提高业务办理效率，简化审核流程来提高金融服务的整体效率；通过互联网、手机APP等线上方式保障基本金融服务畅通。在疫情期间主要采取线上的方式办理各类金融业务并简化相关的业务流程，**但个人金融信息审核的流程不应被简化，仍应在客户身份识别机制下实行严格审核**，在疫情期间保障金融安全。

（二）建议金融科技公司加强对金融平台上发布各类信息审核力度及平台安全性的维护，防止疫情期间不法分子利用互联网及电信设施进行诈骗。

根据监管部门的通知，在疫情期间，大量的金融业务都转为线上处理，金融科技公司需要处理审核的业务量增大，金融科技公司的工作压力也随之增大，在处理金融业务时不仅要加强对客户个人金融信息的保护，更要加强对金融平台上所发布信息的甄别，避免虚假不实信息造成社会恐慌，影响金融安全。同时，由于疫情的影响，消费者个人、制造业、小微企业、民营企业承担了一定的财务压力，金融科技公司应注意加强对平台信息审核及核查，防止不法分子利用平台发布不良、不实信息进行金融诈骗。

（三）建议金融科技公司采用访问控制、加密等安全措施，防止数据泄露、丢失、未经授权被他人使用。

疫情期间，金融科技公司应加强管理用户认证和访问控制的流程，对数据和系统的访问需经相应的认证后方可进入。限制工作人员敏感信息的访问，严格限制对数据库操作的权限，避免金融数据被不法分子利用，扰乱社会秩序。