金融数据安全问题浮出水面 筑起“城墙”严阵以待

或许是因为受到网约车围剿战和外卖混战的影响，滴滴需要开拓一个新的盈利渠道；也或许是对消费金融，滴滴早已悄悄布局。近日，滴滴新上线了一款名为“滴水贷”的在线信贷产品，正式进军消费金融领域。

现在国内的互联网金融是异常火爆，阿里的支付宝、借呗、花呗、蚂蚁金服，腾讯的微粒贷、京东的京东白条，几大互联网巨头都已布局完成。此外，国内从事互联网金融的中小企业数不胜数，再加上传统银行开始拥抱互联网技术并发力场景消费端。在线借贷、在线支付越来越频繁，互联网金融的数据安全问题逐渐浮出水面，引起业内人士的广泛关注。

当下互联网金融面临的威胁

1.数据泄露

据国家互联网金融安全技术专家委员会发布的《互联网金融网站漏洞分析报告》数据显示，在检测分析的1529家互联网金融平台网站中，共发现漏洞7210个，其中高危漏洞451个，占比6.2%，中危漏洞3395个，占比47.1%。跨站脚本、PHP版本不提供安全补锻SQL注入成为排名前三的高危漏洞，这些漏洞不仅能窃取网站用户的密码等私密数据，还可能损害数据库的完整性和暴露敏感信息。

例如，2015年4月22日，国内社保系统存在大量高危漏洞，数千万人员的身份证、财务、薪酬、房屋等敏感信息被泄露。2015年6月，工商银行快捷支付存在严重漏洞，多位北京地区的工行储户存款被盗。

2.数据遭窃

金融网站的技术漏洞和黑客攻击都不是最可怕的，最可怕的是一些内部从业人员在利益的驱使下，也可能会出现从内部窃取数据或越权操纵，导致安全堡垒从内部被攻破。例如，2014年1月支付宝被爆出有内部人员“泄密”超过20G的海量用户信息，而这些信息是其内部员工在后台下载并用来售卖的。在日常生活中，我们的手机、电子邮件等通信工具也会不时地会收到打包出售“厂长与总经理信息库”、“您可能感兴趣的会员”等客户信息的广告。

3.法律法规不健全

由于中国互联网金融发展时间较短，金融市场内现有的证券法、银行法、保险法等都是在传统金融模式的运营下制定的，面对互联网金融相关的金融创新产品，约束力不强，不能有效地适用于这一新生事物的需要，对大数据征信数据处理的各环节及个人隐私等问题未定义明确界限，一旦出现纠纷，也不知如何恰当处理。

可采取的风险控制措施

1.数据加密与反欺诈

为保障金融数据的安全性，从数据产生、传输、处理、交换、到存储和处置的全过程必须保证其完整性、一致性、真实性和保密性。其中，数据加密是信息安全的核心，也是金融数据信息安全的关键属性之一。通过应用加密技术，重要信息数据的保密性、 完整性、可用性以及抗抵赖性能够得到有效保证。

另一方面，反欺诈也是控制信息安全风险的重要举措。近年来，国际先进金融机构把金融理论、统计分析技术和信息技术等结合起来，不断完善反欺诈的定量管理技术。

2. 完善金融统计体系

部分金融活动游离于金融统计体系外，金融业基础数据存在不健全现象。在新的金融业态下，金融创新层出不穷，想要随时动态识别新风险点难度不小。以互联网金融行业为例，部分从业机构尚未接入国家金融信用信息基础数据库，相关经营状况游离于国家金融统计体系外。这些都给金融业综合统计工作造成很大困难，需从制度上尽快完善。

3.完善互联网金融监管和法律体系

互联网金融时代的金融信息安全必须通过立法加以提升，要依靠法律治理，做到有法可依。与国际接轨，借鉴国外信息安全的法律法规，结合我国实际情况，建设坚固可靠的大数据金融法律体系，进一步稳定我国的大数据金融市场。

同时，制定互连网金融的部门规章和行业标准，完善自身监管。互联网金融不仅与金融业有关，还涉及到数据搜集、数据处理、数据交易等各个方面，对客户信息及隐私安全提供切实有效的保护。

4.推进信息安全设备国产化进程

信息安全的攻防永远没有止境，只有创新才是永恒的解决方案。我国建立独立自主的金融信息安全体系刻不容缓，降低金融风险，否则受制于人的被动局面不会轻易改变。推进信息安全设备国产化进程，要从两方面入手：硬件方面，保证硬件环境能够高效安全的运行；软件方面，实现网站安全访问，采取多重信息验证，完善数据加密算法、安全密钥等保障措施。

5. 提高自身信息保护意识

在互联网金融时代，第三方支付平台增大了客户操作风险，并提高了信息被盗的可能性。因此，应当通过印制专门的宣传折页等方式加强对客户信息保护的宣传力度，利用广播、新闻、网络等媒体提高客户自我信息保护意识，不定期通过手机短信或电子邮件的方式为客户发送网银安全使用措施来培养客户良好的操作习惯和风险识别能力。同时，客户要学会使用自身权利，通过举报、投诉等方式客观地对企业进行外部监督

来源：中国反洗钱研究中心网站