

我国互联网金融的特殊风险及防范研究

■ 广东金融学院 杨群华

摘 要: 将互联网技术拓展到金融行业, 可以扩大金融服务的边界和市场, 但互联网金融的发展也使得相应的技术风险、业务风险和法律风险更加凸显, 加大了金融管理部门调控和监管的难度。本文研究认为, 我国需从建立健全互联网金融的安全体系、风险管理体系、法制体系和监管体系入手, 以防范互联网金融的特殊风险。

关键词: 金融科技; 风险管理; 互联网金融; 技术风险; 业务风险; 法律风险

一、引言

互联网金融是依托互联网提供的金融服务与金融产品所形成的虚拟金融市场, 广义的互联网金融还包括互联网金融服务提供的实体金融机构以及相关的法律法规等。

互联网技术的应用使得互联网业与金融业日渐融合, 产生了互联网金融, 并逐渐演变成一个新的金融行业, 对传统的金融组织体系和金融市场体系产生了巨大影响。近年来, 我国互联网金融高速发展, 宜信、拍拍贷、红岭创投、畅贷网、人人贷、团贷网等人对人对款(简称P2P贷款)网络信贷平台快速发展, 腾讯、京东商城、慧聪网等互联网科技公司纷纷进入小额贷款领域, 建设银行、工商银行、国开行与阿里巴巴或金银岛等平台合作, 开展“网络贷”、“e单通”等互联网金融业务。2012年6月, 建设银行自建电子商务平台“善融商务”, 希望凭借该平台上积累的交易数据进行数据挖掘, 进而开发金融产品; 2013年2月, 阿里巴巴、中国平安、腾讯等9家公司筹建的众安在线财产保险公司获得保监会的批复, 成为开展专业网络财险公司的试点; 2013年3月, 阿里巴巴集团宣布筹建阿里小微金融服务集团, 负责阿里巴巴集团旗下所有面向小微企业以及消费者个人服务的金融业务。

将互联网技术拓展到金融行业, 极大地降低了金融交易的时间和成本, 扩大了金融服务的边界和市场。

但是, 互联网金融的虚拟化、高科技化、跨国经营的特点以及监管法律法规缺位等问题, 也导致其风险管理比传统金融更加复杂, 对维护我国金融稳定提出了更大的挑战。

二、互联网金融的特殊风险

作为互联网技术与金融全面结合的产物, 互联网金融不但面临传统金融活动中存在的信用风险、流动性风险和市场风险, 还面临由互联网信息技术引起的技术风险、由虚拟金融服务引起的业务风险以及由法律法规滞后引起的法律风险。

(一) 系统性的技术风险

1. 系统性的安全风险

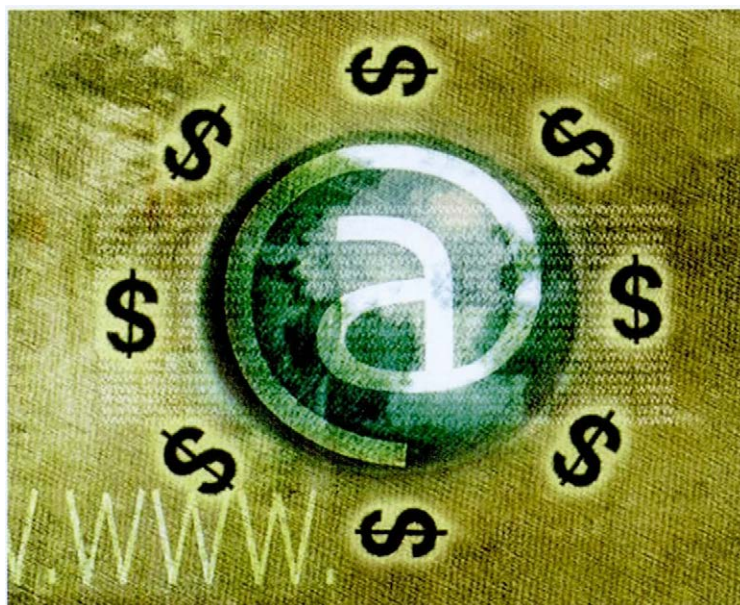
互联网金融依托发达的计算机网络开展, 相应的风险控制需由电脑程序和软件系统完成。因此, 计算机网络技术是否安全与互联网金融能否有序运行密切相关, 计算机网络技术也成为互联网金融最重要的技术风险。互联网传输故障、黑客攻击、计算机病毒等因素, 会使互联网金融的计算机系统面临瘫痪的技术风险。

一是密钥管理及加密技术不完善。互联网交易的运行必须依靠计算机来进行, 交易资料都存储在计算机内, 并通过互联网传递信息。然而, 互联网是一个开放式的网络系统, 在密钥管理及加密技术不完善的情况下, 黑客可以在客户机传送数据到服务器的过程中进

行攻击,甚至攻击系统终端,给互联网金融的发展造成危害。

二是TCP/IP协议的安全性较差。目前互联网采用的传输协议是TCP/IP协议族,这种协议在数据传输过程中力求简单高效,注重信息沟通通道畅通,但没有深入考虑安全性问题,导致网上信息加密程度不高,在传输过程中容易被窥探和截获,引起交易主体的资金损失。

三是病毒容易扩散。互联网时代,计算机病毒可通过网络快速扩散与传染。一旦某个程序被病毒感染,则整台计算机甚至整个交易网络都会受到该病毒的威胁,破坏力极大。在传统金融业务中,安全风险只会带来局部的影响和损失,在互联网金融业务中,安全风险可能导致整个网络的瘫痪,是一种系统性的技术风险。



2. 技术选择风险

互联网金融技术解决方案是开展互联网金融业务的基础,但选择的技术解决方案可能存在设计缺陷或操作失误,这就会引起互联网金融的技术选择风险。技术选择风险可能来自于信息传输过程,也可能来自于技术落后。

一是信息传输低效。如果从事互联网金融业务的机构选择的技术系统与客户端软件的兼容性差,就可能在与客户传输信息的过程中出现传输中断或速度降低,延误交易时机。

二是技术陈旧。如果从事互联网金融业务的机构选择了被淘汰的技术方案,或者技术创新与时代脱节,就有可能出现技术相对落后、网络过时的状况,导致客户或从事互联网金融业务的机构错失交易机会。在传统金融业务中,技术选择失误一般只会导致业务流程缓慢,增加业务处理成本,但在互联网金融业务中,信息传输速度对市场参与者能否把握交易机会至关重要,技术选择失误可能导致从事互联网金融业务的机构失去生存的基础。

3. 技术支持风险

由于互联网技术具有很强的专业性,从事互联网金融业务的机构受技术所限,或出于降低运营成本的考虑,往往需要依赖外部的技术支持来解决内部的技术问题或管理难题。在互联网技术飞速更新换代的今天,寻求外部技术支持或者是技术外包是发展互联网金融业务的必然选择,有助于提高工作效率。然而,外

部技术支持可能无法完全满足要求,甚至可能由于其自身原因而中止提供服务,导致从事互联网金融业务的机构无法为客户提供高质量的虚拟金融服务,进而造成互联网金融的技术支持风险。

另一方面,我国缺乏具有自主知识产权的互联网金融设备。目前使用的互联网金融软硬件设施大都需要从国外进口,对我国的金融安全形成了潜在威胁。

(二) 包含计算机系统和交易主体的业务风险

1. 操作风险

互联网金融业务的操作风险可能来源于互联网金融的安全系统,也可能是因为交易主体操作失误。从互联网金融的安全系统来看,操作风险涉及互联网金融账户的授权使用、互联网金融的风险管理系统、从事互联网金融业务的机构与客户的信息交流等,这些系统的设计缺陷都有可能引发互联网金融业务的操作风险。从交易主体操作失误来看,如果交易主体不了解互联网金融业务的操作规范和要求,就有可能引起不必要的资金损失,甚至在交易过程中出现流动性不足、支付结算中断等问题。由于互联网金融服务方式的虚拟性,互联网金融的经营活动打破了传统金融业务的网点限制,具有明显的地域开放性。在互联网金融业务中,安全系统失效或交易过程中的操作失误,都会构成互联网金融发展过程中的风险累积,对全国乃至全球金融网络的正常运行和支付结算产生影响。

2. 市场选择风险

互联网金融的市场选择风险是指由于信息不对称

导致从事互联网金融业务的机构面临不利选择和道德风险而引发的业务风险。一方面, 互联网金融业务和服务提供者都具有显著的虚拟性, 相应的业务活动大都在由电子信息构成的虚拟世界中进行, 增加了确认交易者身份、信用评价等方面的信息不对称性。在实际业务中, 客户可能利用他们的隐蔽信息作出不利于互联网金融服务提供者的决策, 而从事互联网金融业务的机构却无法在网上鉴别客户的风险水平, 导致其在选择客户时处于不利地位。

另一方面, 在信息不对称的情况下, 互联网金融市场可能成为“柠檬市场”。互联网金融服务是一种虚拟的金融服务, 加之我国的互联网金融还处于起步阶段, 客户不了解各机构提供的服务质量, 这就有可能导致价格低, 但服务质量相对较差的互联网金融服务提供者被客户接受, 而高质量的互联网金融服务提供者却因价格偏高被挤出互联网金融市场。

3. 信誉风险

信誉风险是指从事互联网金融业务的机构没有建立良好的客户关系, 没有树立良好的信誉, 导致其金融业务无法有序开展的风险。无论是传统金融机构还是互联网金融服务提供者, 信誉风险的消极影响都是长期持续的。信誉风险不仅会使公众失去对互联网金融服务提供者的信心, 还会使互联网金融服务提供者同客户之间长期建立的友好关系受到损害。由于互联网金融业务采用的多是新技术, 更容易发生故障, 任何原因引起的系统问题都会给互联网金融服务提供者带来信誉风险。一旦从事互联网金融业务的机构提供的金融

服务无法达到公众的预期水平, 或者安全系统曾经遭到破坏, 都会影响互联网金融服务提供者的信誉, 进而出现客户流失和资金来源减少等问题。

(三) 法律风险

互联网金融的法律风险主要包括两个方面: 一是互联网金融业务违反相关法律法规, 或者交易主体在互联网交易中没有遵守有关权利义务的规定, 这类风险与传统金融业务并无本质差别; 二是互联网金融立法相对落后和模糊, 现有的银行法、证券法、保险法等法律法规都是基于传统金融业务制定的, 不适应互联网金融的发展。

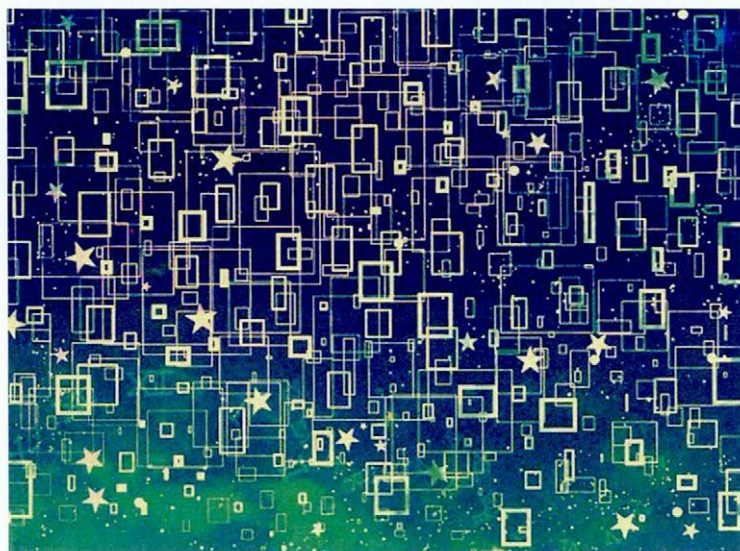
我国的互联网金融还处于起步阶段, 相应的法律法规还相当缺乏。近年来, 我国相继出台了《电子签名法》、《网上银行业务管理暂行办法》、《网上证券委托管理暂行办法》、《证券账户非现场开户实施暂行办法》等法律法规, 但这些法律法规也只是基于传统金融业务的网上服务制定的, 并不能满足互联网金融发展的需求, 而互联网金融市场的准入、资金监管、交易者的身份认证、个人信息保护、电子合同有效性的确认等方面都还没有明确的法律规定。因此, 在利用互联网提供或接受金融服务时, 配套法规的缺乏容易导致交易主体间的权利、义务不明确, 增加相关交易行为及其结果的不确定性, 导致交易费用上升, 不利于互联网金融的健康发展。

三、互联网金融风险的防范策略

在互联网金融中, 经济活动表现为货币信息的传递与调拨, 代表货币资金的数字化信息在网络内流动。“虚拟”的金融交易不受时间和地域的限制, 使得金融风险的传播速度加快、波及范围扩大。此外, 互联网金融业务几乎全部在网上完成, 交易对象不明确、交易过程透明度低, 都加剧了金融管理部门调控和监管的难度。由此可见, 互联网金融业务对金融风险具有放大效应, 必须加强风险防范与管理。

(一) 构建互联网金融安全体系

一是改进互联网金融的运行环境。在硬件方面加大对计算机物理安全措施投入, 增强计算机系统的防攻击、防病毒能力, 保证互联网金融正常运行所依赖的硬件环境能够安全正常地运转; 在网络运行方面实现互联网金融门户网站的





安全访问,应用身份验证和分级授权等登录方式,限制非法用户登录互联网金融门户网站。

二是加强数据管理。将互联网金融纳入现代金融体系的发展规划,制订统一的技术标准规范,增强互联网金融系统内的协调性,提高互联网金融风险的监测水平;利用数字证书为互联网金融业务的交易主体提供安全的基础保障,防范交易过程中的不法行为。

三是开发具有自主知识产权的信息技术。重视信息技术的发展,大力开发互联网加密技术、密钥管理技术及数字签名技术,提高计算机系统的关键技术水平和关键设备的安全防御能力,降低我国互联网金融发展面临的技术选择风险,保护国家金融安全。

(二) 健全互联网金融业务风险管理体系

一是加强金融机构互联网金融业务的内部控制。互联网金融业务的本质仍然是金融风险,从事互联网金融业务的机构应从内部组织机构和规章制度建设方面着手,制定完善的计算机安全管理方法和互联网金融风险防范制度,完善业务操作规程;充实内部科技力量,建立专门从事防范互联网金融风险的技术队伍。

二是加快社会信用体系建设。完善的社会信用体系是减少信息不对称、降低市场选择风险的基础。以人民银行的企业、个人征信系统为基础,全面收集非银行信用信息,建立客观全面的企业、个人信用评估体系和电子商务身份认证体系,避免互联网金融业务提供者因信息不对称作出不利选择;针对从事互联网金融业务的机构建立信用评价体系,降低互联网金融业务的不确定性,避免客户因不了解金融机构互联网金融业务的服务质量而作出逆向选择。

(三) 加强防范互联网金融风险的法制体系建设

一是加大互联网金融的立法力度。及时制定和颁发相关法律法规,在电子交易的合法性、电子商务的安全性以及禁止利用计算机犯罪等方面加紧立法,明确数字签名、电子凭证的有效性,明晰互联网金融业务各交易主体的权利和义务。

二是修改完善现行法律法规。修订现有法律法规中不适合互联网金融发展的部分,对利用互联网实施犯罪的行为加大量刑力度,明确造成互联网金融风险应承担的民事责任。

三是制定网络公平交易规则。在识别数字签名、保存电子交易凭证、保护消费者个人信息、明确交易主体的责任等方面作出详细规定,以保证互联网金融业务的有序开展。

(四) 建立互联网金融监管体系

一是加强市场准入管理。将是否具有相当规模的互联网设备、是否掌握关键技术、是否制定了严密的内控制度、是否制定了各类交易的操作规程等内容作为互联网金融市场的准入条件,对互联网金融各种业务的开展加以限制和许可;根据开办互联网金融业务的主体及其申报经营的业务,实施灵活的市场准入监管,在防范金融风险过度集聚的同时,加大对互联网金融创新的扶持力度。

二是完善监管体制。互联网金融市场的发展突破了银行业、证券业、保险业分业经营的界限,对分业监管模式提出了很大挑战。我国应协调分业与混业两种监管模式,对互联网金融风险实行综合监管;互联网金融的发展打破了地域限制,对单独的国内监管提出了挑战,我国需与有较高互联网金融风险防范能力的国家和机构合作,学习对方的先进技术,对于可能出现的国际司法管辖权冲突进行及时有效的协调。FTI

参考文献:

- [1]冯静生.网络金融风险:我国的监管状况及完善对策[J].金融教学与研究,2009,(1):41-44.
- [2]谢平,邹传伟.互联网金融模式研究[J].金融研究,2012,(12):11-12.
- [3]张玉喜.网络金融的风险管理研究[J].管理世界,2002,(10):139-140.