我国第三方支付信息安全风险研究

卓武扬[1] 胡阿思[2] 宫兴国[3] 陈 婷[4]

(1. 上海第二工业大学经济与管理学院 上海 200000;
2. 襄城县委办公室 河南襄城 461700;
3. 中国人民银行济宁市中心支行 山东济宁 272000;
4. 西华大学经济学院 四川成都 610039)

摘 要:[**目的/意义**]我国第三方支付在快速发展的同时,信息安全风险也日益涌现,不仅导致了交易各方的权益受损,也增加了风险管控的难度,对信息安全风险的研究有助于规范企业合法运营,保护消费者合法权益。[**方法/过程**]在现有研究的基础上,分析信息安全风险产生的原因,通过构建指标体系对不同层面的信息安全风险进行评估。[**结果/结论**]法律、平台和技术风险情况对第三方支付的信息安全风险影响较大,用户自身风险对其影响较低。因此,我国第三方支付信息安全风险防范应创新管制思路、增强平台内控管理能力、提高企业技术手段、完善纠纷解决及救济机制,为第三方支付市场提供健康的发展环境。

关键词:第三方支付;信息安全风险;第三方支付企业;风险分析;风险评估
中图分类号:F830 **文献标志码:**A **文章编号:**2095-1124(2019)06-0042-20

伴随着互联网金融的创新发展、电子商务的模式变化、移动通讯工具的更新换代,在保障资金安全且信息保密的前提下,消费者在交易时更倾向于使用移动支付模式[1]。在此背景下,第三方支付应运而生,发挥着类似银行、信用卡等信用机构的作用,主要目的是用来解决买卖双方的信用问题[2]。我国第三方支付行业发展迅猛,2017年第二季度和第三季度的第三方支付交易规模达27.1万亿[3]和31.6万亿[4],面对可见的利润空间,使得许多第三方支付企业趋之若鹜,纷纷进军此行业或不断扩大企业规模。然而,2017年仅有247家第三方支付企业获得牌照[5],面对激烈的市场竞争,第三方支付企业的发展进入了"野蛮生长的时代",各种金融风险层出不穷。

其中最具突出的和最具有代表性的是信息安全风险,与传统的商业银行业务相比,依托网络进行的支付交易更容易留下浏览记录,泄露个人信息,为不法分子盗取个人信息提供了通道。不管是支付宝2018年度账单事件,还是携程用户2014年的支付信息安全事件等各类支付平台的信息安全事件,无一不暴露出当前的网络支付信息保护系统存在漏洞,导致用户个人信息泄露,继而造成人身、财产权益受到损害,使消费者与第三方支付平台之间的矛盾日益凸显。此外,用户自身信息保护意识较弱,再加之自身举证困难,凭一己之力根本无法查明信息泄露的原因,也没有太多的权力诉求渠道帮助消费者维护自身权益。

2016年全国人大常委会发布的《中华人民共和国网络安全法》中明确提出要维护网络运行安全,制定网络安全的长远战略目标,进一步规范各级政府、部门的责任和权力,提高政策、政务的透明度、开放性,加大对违法犯罪行为的惩罚力度。该项法案虽然完善了网络安全方面的具体义务和责任,但还不能满足个人信息安全保护方面的法律需求,当前并未出台一部专门针对每一个体的信息安全保护法,现行的法律条款数量有

收稿日期:2019-06-11
作者简介:卓武扬(1975—),男,教授,经济学博士,金融学博士后、民商法学博士后,研究方向为金融制度、金融监管;胡阿思(1993—),女,管理学硕士,研究方向为公司金融;宫兴国(1971—),男,经济师,研究方向为金融学、经济学;陈婷(1995—),女,硕士研究生,研究方向为金融学。

限,使用范围相对狭窄,没有对消费者个人的信息安全起到有效的保护作用。所以,要保护消费者的信息安全权益,需要对第三方支付的信息安全风险进行科学合理的评估。基于此,本文在已有学者研究的基础上,具体研究这一风险产生的原因,识别、分析信息安全风险的类型,并通过构建指标体系进行分析,分别从法律、平台、技术和用户自身角度进行定量和定性分析,探讨不同风险的等级及影响因素,针对存在的风险对象提出合理的意见和建议,丰富和完善第三方支付领域风险防范措施。

1　文献综述

第三方支付伴随着互联网金融的飞速发展,给我们的生产、生活带来方便的同时,也潜藏着诸多风险,尤其是信息安全方面,是学者们热议的问题之一。

关于互联网金融信息安全风险的研究中,学者们主要从信息安全技术、系统漏洞等方面进行研究。如毕建华、肖林江(2016)指出我国互联网金融行业存在诸多问题,尤其是网络平台的信息安全防护机制尚不成熟,加之新型的信息安全风险频出,这都得使互联网金融行业信息安全风险面临诸多挑战[6]。刘杰(2015)从信息安全角度分析整个互联网金融风险,提到客户安全认证风险、信息通信风险、系统漏洞风险、数据安全风险等方面是目前互联网金融机构面临的最大的风险隐患,要深入分析其背后隐藏的风险成因,实施相应的防范措施[7]。冯国震(2018)将金融企业的信息安全管理与风险控制相链接,提出信息安全的木桶效应,强调要尤为重视技术操作类风险和信息安全管理类风险[8]。郑志伟(2014)提到我国互联网金融行业还处于起步阶段,安全策略不完善,安全管理水平低,各种客户信息泄露事件频发,完善网络安全体系建设,用户要使用安全的支付方式[9]。陈哲谦(2016)通过对互联网金融信息安全风险进行评估,得出风险值与资产的脆弱性和控制措施相关,提出要有限使用国产软硬件,加强信息风险监控[10]。

关于第三方支付交易过程中存在的信息安全风险,国内外学者主要倾向于法律监管、企业内部控制和全社会的安全风险意识等方面。如 Wu Y (2010)用标准化方法分析第三方支付发展中存在的问题,认为应重视第三方支付发展中存在的风险,并采取加大监管,完善法律等措施[11]。Sullivan R J(2014)指出政策制定者需要一个广泛的视角来判断支付诈骗方法,提高支付安全性[12]。刘春晓(2015)通过对我国境内、我国港澳地区、欧盟和美国的个人信息保护法规深入研究、比较分析,得出政府主管部门应加强立法建设,并加大执法力度,呼吁全社会重视个人信息安全,这样才能为网络支付的发展创造一个稳定健康的环境[13]。张鹏(2018)通过对第三方支付平台运营模式研究,分析得出目前我国第三方支付平台信息安全所面临的主要问题是支付平台信息安全法律不完善且准入门槛过低,导致用户信息隐私权益难以保护[14]。杨亦军、谭晟(2010)着重分析了第三方支付企业自身存在的信息安全风险,包括企业内部控制机制、技术漏洞等风险,提出要通过加强系统应用风险的防范能力和内部控制管理能力,最大限度地减少系统的运行风险,保障国家金融安全[15]。毕娟、陈博(2018)提到我国大部分网站隐私保护政策内容不科学、不合理,设置免责条款过多,虽然我国于 2017 年先后出台《网络安全法》《个人信息保护法》,但遭遇到某些权力保护时仍然没有起到有效的约束力[16]。谢迎春(2017)主要分析了发达国家在顶层设计、监管协调机制方面对第三方支付信息安全的主要做法,以启示我国创新支付机构的信息保护监管理念和行为方式[17]。谭超、赵丽霞、张岚(2016)通过对第三方企业内部管理模式的实证研究,创新性地评估各因子的影响程度,提出具体的方法改进和完善企业管理制度[18]。王思平、李奔(2018)深入研究了移动支付中隐藏的风险,指出木马和病毒风险、钓鱼欺诈风险、个人信息泄露风险是目前网络安全支付所面临的最主要风险形式[19]。陈丽莉(2013)采用威胁树方法对信息安全进行了实证评估,并对非法访问账户、支付过程付款账户被篡改等风险进行了分析[20]。Joshi M,

Singh V K(2017)通过评估数据安全漏洞和感知风险对消费者购买决策的影响,得出第三方支付安全的重要性[21]。

通过对文献的梳理,发现第三方支付企业存在着诸多风险,本文着重探讨第三方支付信息安全方面的风险,运用层次分析法(The analytic hierarchy process,简称 AHP),即结合定量和定性的分析方法,多维度、多层面对信息安全风险进行评估,计算出每个指标对信息安全风险的影响程度,根据结论有针对性地提出信息安全风险的防范措施和第三方支付企业的发展方向。

2 信息安全风险成因分析

在交易过程中,有相关法律法规的规范力和社会道德的约束力对用户信息安全起到保护作用,但实际交易中,因平台系统故障、用户私密信息被盗取或操作失误等行为导致消费者权益遭受损失时,并没有明确的管制措施来限定各方权责,也没有正式的权力诉求渠道来保护消费者合法权益,从而使消费者和第三方支付企业之间形成一种不对等的交易关系。因此,我们从社会、法律、第三方支付企业和用户自身四方面对信息安全风险成因进行具体分析,以便更好地防范和化解这一风险。

2.1 社会视角:网络安全技术的发展滞后

截至 2017 年 12 月,我国网民规模达 7.72 亿,手机网民规模达 7.53 亿,互联网普及率达 55.8%①,超过了全球平均水平,说明我国已成为互联网技术应用的实践先锋。随着互联网应用的深化,虚拟交易的不断发展,网络病毒数量日益增长,病毒类型也日益多样化。2018 年上半年瑞星“云安全”系统共截获病毒样本总量 2587 万个,病毒感染次数 7.82 亿次,新增木马病毒占总体数量的 62.83%;共截获手机病毒样本 345 万个,新增病毒类型以信息窃取、资费消耗等四类为主,其中信息窃取类病毒占比 28%,位居第一②。面对多变复杂的网络安全现状和民众日益增长的安全业务需求,我国目前的网络安全技术尚不能完全解决,它不仅威胁着消费者的信息安全,网络安全国际合作也有待进一步加强。

2.2 法律视角:个人信息的法律保护方面尚未完善

2017 年 3 月和 6 月,我国先后出台的《民法总则》和《网络安全法》中对消费者个人的信息安全保护更加明确和规范,是个人信息法律法规体系建设的一大进步,当消费者权益受损时,可以更好地诉诸于法律武器来保护自身合法权益。但是,对于消费者个人隐私权的保护,比如信息删除权和被遗忘权等仍缺少具体的法律依据,对于维权渠道、权责认定、赔偿方式等问题的解决,也缺乏可操作性。我国尚未出台《个人信息安全保护法》,对个人信息的完整性保护方面存在很大的局限性,法律法规重“刑事处罚”和“行政管理”,轻“民事确权”与“民事归责”,导致用户信息遭受损害后,侵权方会受到刑事或行政处罚,而未对消费者个体的经济或非经济损失进行补偿。所以,我国急需出台《个人信息安全保护法》及相关配套措施来进一步保障用户的信息安全。

2.3 第三方支付企业视角:平台自身管理不规范

第三方支付企业为了保证网上交易支付的安全性,需企业在每个环节上都采取相应的技术手段,对用户数据的完整性加以控制,对用户个人信息的验证方式加以防范,以降低双方交易风险,保证网络交易的安全进行。而企业是以营利为目的的组织,为了获得竞争优势和盈利,第三方支付企业可能会选择压缩信息安全管理方面的资金投入,减少人才培养,导致企业内部技术落后、管理混乱,从而使用户交易不畅或泄露个人信息,因此,要引起第三方支付企业自身的重视,在信息安全管理方面要改善投入方式、加大投入力度。

2.4 个人视角:用户自身风险意识不强

当今中国互联网金融的发展,网络消费、网上交易已经成为民众生活不可或缺的一部分,随着各种网络平台的异军突起,用户注册账号、设置密码或进行密码保护的频率更多,这使民众更多地注重个人敏感信息的保护(如身份证号、银行卡密码等信息)而忽略了个人信息的整体保护,如很少人会认真阅读平台上所有产品的服务协议、有些人会随意允许开通该平台设置的所有权限(定位服务等),殊不知,这些简单的行为可能会潜伏着巨大信息安全风险。因此,用户个人应加强个人信息的风险意识,不给不法分子以可乘之机。

3 信息安全风险的类型分析

根据我国互联网金融的发展态势和第三方支付行业信息安全风险的典型特征,本文将信息安全风险主要划分为四大类别,即法律风险、平台自身风险、技术漏洞风险和用户自身风险。各个类别的风险具体分析如下。

3.1 法律风险

3.1.1 政策法规的约束力

政府的相关政策法规约束力方面是政府未及时发挥自身作用和健全各项法律法规,从而未对相关企业及社会形成强有力的监督。所以,网络交易时要清晰界定各方权力与义务,对违反法律、法规或各项规章制度及未按规定履行义务的一方给予处罚。

第三方支付的政策法规主要是规范第三方支付企业及企业员工的行为规范和准则,从信息安全法律的框架出发主要包括以下三方面:一是网络系统的日常维护层面风险,包括要规范系统安全的运行范围,防止企业未经授权或超出授权范围的不法经营,还应制定企业的网络日常运行制度;二是应急措施制度层面风险,包括应急处理能力和灾后恢复处理能力,确保支付业务的连续性;三是用户隐私保密制度层面风险,包括设立保密等级,制定保密制度等。政策法规的完善、信息安全等级体系的构建要与传统金融机构有所区别,要形成一个制度的保障。

3.1.2 非正式制度的规范力

非正式支付的规范力包括社会的道德选择、行业监管风险及第三方支付企业的注册协议、服务条款等方面。一方面,互联网金融和第三方支付行业还处于发展初期,行业协会这种非正式的组织形式是政府和企业沟通的重要桥梁,但并未有规范的政策标准进行统一约束,没有形成自律组织约束、协会成员自我约束的标准,整个行业存在不合规运营所带来的风险。另一方面,第三方支付企业在政府政策的扶持和引导下,合理规范企业行为,但可能存在未准确把握行业定位、及时识别和控制信息安全、没有为消费者提供合法权益保护而产生的诸多风险。

3.2 平台自身风险

3.2.1 运行风险

平台运行风险是指第三方支付平台在处理大流量操作时突然无法正常运行,且无有效的应急措施而产生的风险。平台的运行系统在设计之初只是满足基本的交易,但随着业务范围的不断扩大,用户数量的增多,平台的访问人数、交易量及交易额都会大幅增长,这就超出了系统预设的处理范畴,导致系统运行不稳、造成交易风险。此外,当系统故障时,而又缺乏紧急处理机制,未能及时有效进行软硬件维修、故障排除,可能造成系统瘫痪、平台运行中止,消费者的信息安全将遭受巨大影响。

3.2.2 内部控制风险

第三方企业内部控制是指平台总体的内部管理水平,包括建设内部控制的规章制度、具体执行程序以及

对外服务管理等方面。平台在不断对外扩展业务的过程中,往往更重视技术的改性和平台的吸引力,而忽视了企业内部的安全管理,各方面的管理制度模糊,未严格明晰部门工作内容和每位员工的权责范围,易导致对客户账户信息的维护不善,将带来数据泄密的风险,造成平台信息的安全隐患,也会影响第三方支付企业的信用度。

3.2.3 操作风险

操作风险的产生来源于两个方面:一是错误操作,二是恶意操作。第三方支付企业内部员工或用户自身都可能存在此类风险。

错误操作情况在现实交易中最为常见,从企业角度来看,随着企业业务范围的持续增加,企业日常安全运营的各项成本逐渐提高,当然,也包括人力成本,企业出于节约预算成本的目的或短时间内未找到合适的人员配置等原因,导致人员配比与企业信息安全发展之间的矛盾,进而导致员工少、工作多的情况成为常态,极有可能出现员工由于疏忽而误操作的情况。另外,员工对工作内容不熟悉,且未能及时参与企业的各项培训,也可能导致业务操作风险。从用户自身角度来讲,可能存在缺乏网络安全常识或安全意识不强而导致的操作风险,这都将危及第三方支付业务的总体安全。

恶意操作是因为计算机终端的安全保护配置不当或服务器管理不善而给不法分子以可乘之机,植入计算机病毒,盗取用户所有的信息资料。究其原因,可能是操作系统基本来源于国外发达国家、企业内部安全管理问题、亦或平台外的不法分子恶意操作,使用户信息安全遭受威胁。

3.3 技术漏洞风险

3.3.1 网络身份认证风险

相比于传统的金融交易,互联网时代的交易形式发生了根本性的变化,取代了面对面的交易方式,双方整个交易过程都在网上进行,远程识别、确认相关信息等内容,因而无法确定对方的合法身份,增大了信息的安全风险。当今互联网金融的发展,使大数据、云计算等互联网技术广泛应用,但缺乏信用体系建设和有效的网络身份认证技术来保证登陆用户身份的唯一性,会使得一些不法分子通过相关网络渗透技术,窃取用户信息,实施违法犯罪行为。

3.3.2 数据安全风险

数据的开放、共享是大数据时代的发展方向,也是第三方支付行业的发展基础。通过对数据的挖掘、整理和分析,可了解用户的信用情况、购买偏好等相关信息,为用户提供针对性、多样化的服务和产品。但是,正因为数据具有极大的经济价值,更容易遭受黑客攻击。数据安全的风险主要体现在两方面:数据存储的安全和传输过程的安全。第三方支付企业对个人信息的保密性、传输系统安全性并不完善,安全产品配置不当,没有数据输入、输出的监控审计技术,导致企业的防护、监管措施不足,不能起到预期的信息保护作用,可能使用户隐私、客户合法权益受到威胁。

3.3.3 客户端安全认证风险

客户端安全认证风险是指用户的客户端(PC 或移动设备)在遭受病毒或被恶意第三方插件攻击后,不法分子会截获用户的账户、密码、验证码等敏感信息,然后利用诈骗信息,在未经用户客户端安全认证的情况下,通过网络浏览记录或其他方式,窃取用户的敏感信息和平台资金。随着互联网技术的发展,获取用户个人信息的方式层出不穷,各种新颖的诈骗手段、新奇的诈骗广告大范围的传播,某些犯罪集团甚至将非法网站设在海外,以躲避国内监管,从而大规模的非法牟利,使用户在毫不知情的状况下上传个人信息而上当受骗。

3.4 用户自身风险

3.4.1 用户自身的信息安全防护意识

用户自身的重要信息泄露,除了第三方支付平台的技术问题和不法分子的非法盗取外,还有用户自身的安全防护意识,主要表现在以下两方面:第一,为了方便记忆,经常用相同的账户和密码在不同的平台登陆,给不法分子以可乘之机,他们会采用黑客技术,与网银、支付宝等平台进行信息匹配登陆,验证有价值的信息,盗取用户平台资金。第二,未使用安全的登陆方式,随意连接公共WiFi,扫描不明二维码,无意识泄露敏感信息等行为,如果被恶意利用,将对用户个人隐私权益构成严重的威胁。

3.4.2 纠纷解决机制、权力救济渠道的诉求

当发生第三方支付账户信息泄露的纠纷时,消费者自身举证困难,凭借个人能力,根本无法查明泄密原因,更不知道通过何种渠道、何种方式进行权力诉求,追究相关责任人的法律责任。我国目前的信息安全纠纷事件频出,但支付机构并未及时、准确处理交易偏差和客户投诉,可能企业并未配有专业的管理部门或人员去履行该义务,也可能是我国的相关监管部门缺乏完善的纠纷解决机制,未能有效地保护消费者的合法权益。

4 信息安全风险指标体系构建与风险评估

现有文献中关于信息安全风险度量都采用定性与定量相结合的方法,一类是采用理论和实例分析方法。如:寿宁静(2018)以2018年支付宝年度账单事件为分析依据,指出第三方支付平台默认勾选某些选项,分享用户数据信息,大大侵害了用户们的个人信息权力[22]。周永战、赵颖坤(2013)通过对第三方支付行业的监管分析,指出信息安全等级保护监管的诸多问题,如检查机构信息系统定级是否准确、是否按照相应等级进行安全管理和技术配备、是否按照要求进行安全有效整改[23]。另一类进行实证分析。如:李雪雯(2018)以四种具体的支付方式为例,通过层次分析论证其支付交易风险[24]。危怀安、李松涛(2018)对第三方支付信息安全监管进行了多元化的调查研究,对第三方支付机构的监管对策和信息安全监管的影响因素进行了实证分析[25-26]。本文基于风险出现的原因和风险类型的分析,以法律、第三方支付企业和用户的信息安全关系为分析对象,更倾向于建立信息安全风险指标体系,采用层次分析法(AHP)对指标权重进行分析。

4.1 指标的选取

第三方支付企业信息安全评估指标的选取是进行风险评估的基础性工作,指标选取具有普遍性、科学性和合理性。本文结合相关文献,将指标体系分为4个一级指标和10个二级指标(见表1)。

表1　第三方支付风险的指标评价体系

目标层	一级指标	二级指标
第三方支付信息安全风险	法律风险	政策法规的约束力
		非正式制度的规范力
	平台风险	运行风险
		内部控制风险
		操作风险
	技术风险	网络身份认证风险
		数据安全风险
		客户端安全认证风险
	用户风险	个人信息安全防护意识
		纠纷解决机制和权力救济渠道

法律风险是从政府和社会角度出发，确保信息安全的基本保障力，它由政策法规的约束力和非正式制度的规范力两个指标组成。政策法规是从政府立法层面出发，通过各项制度、规章予以约束。非正式制度既包括网络、社会道德规范、行业协会组织等非正式的规范作用，还包括第三方支付企业内部制定的各项服务条款、责任声明等保障用户合法权益的协议。

平台风险主要指第三方支付企业所提供交易服务平台自身存在的风险，它包括运行风险、内部控制风险和操作风险。运行风险是指平台突然处理大量交易操作时无法正常运行，且应急处理措施不力而造成的风险。内部控制风险是指第三方支付企业内部管理机制不健全而带来的风险，包括各类制度、规范和措施。操作风险指第三方支付企业内部员工或用户自身存在的操作失误或遭受恶意操作所带来的风险。

技术风险又叫系统漏洞，此类风险与用户信息安全有着最直接的联系，也是第三方支付企业一直在研究和完善的方面。它由网络身份认证风险、数据安全风险和客户端安全认证风险三个指标组成。网络身份认证风险是身份认证的验证密码在传输过程中被木马程序或网络监听设备所截取而带来的风险。数据安全风险指第三方支付企业在存储与传输敏感信息时容易出现客户数据丢失、泄露和被篡改的风险。客户端安全认证风险是指一些不法分子引导客户在钓鱼网站等平台输入支付账户、密码等个人信息，从而导致信息被窃取的风险。

用户风险主要体现在用户自身的信息安全防护意识和对纠纷解决机制、权力救济渠道的诉求上。个人信息安全防护意识指用户是否有意识的保护个人信息，使用安全的登陆方式，按照正确的支付流程进行交易。纠纷解决机制和权力救济渠道指当用户信息安全权受到侵害时，是否及时进行权力诉求，企业是否能据实、准确、及时处理交易差错和用户投诉。

4.2　风险评估的基础工作

4.2.1　数据来源

本文结合指标体系的性质，采取层次分析法（AHP）进行指标体系的权重测算，即对于指标的重要性进行测算。首先利用专家咨询的方式对指标进行统一评分，通过得到的分析结果进行检验，再利用层次分析法（AHP）计算每一层级的指标权重，进而得到合理的指标体系。

数据来源采用调查问卷的形式，受访对象是金融专业人士和互联网金融相关从业人员，利用纸质版和电子版两种方式，问卷发放 70 份，实际反馈 65 份，经统计分析，其中有效问卷 60 份，问卷有效率达到 85%，调查结果可用做研究。

4.2.2　9 级标度法

为了尽可能减少各个指标之间的模糊比较，通过分值的方法量化表示，故采用 1—9 标度方法，对一级指标和二级指标分别进行赋值，得出相应的模糊判断矩阵（见表 2）。

表 2　模糊判断矩阵标度法

标度	含义
1	i，j 同样重要
3	i 比 j 稍微重要
5	i 比 j 比较重要
7	i 比 j 非常重要
9	i 比 j 绝对重要
2、4、6、8	上述判断的中间值
上述标度的倒数	j 对 i 的重要性之比

4.3　第三方支付风险度量

4.3.1　各级度量指标权重

利用问卷收集、分析数据,采用1—9标度法构造模糊判断矩阵,使矩阵中的各数据是同级指标之间的相对比较值。根据调查问卷中显示的一级度量指标比较结果,综合评分的算术平均值,构建判断矩阵,并进行一致性检验,计算结果见表3。

表3　各级指标权重

一级指标	权重	二级指标	权重
法律风险	0.283	政策法规的约束力	0.606
		非正式制度的规范力	0.394
平台风险	0.313	运行风险	0.411
		内部控制风险	0.472
		操作风险	0.117
技术风险	0.276	网络身份认证风险	0.268
		数据安全风险	0.385
		客户端安全认证风险	0.347
用户风险	0.128	个人信息安全防护意识	0.299
		纠纷解决机制和权力救济渠道	0.701

4.3.2 一致性检验

步骤如下:

1)重要性排序。方程为 $U_W = \lambda_{max} \cdot W$,其中 W 是特征向量,λ_{max}是最大特征根。

2)一致性检验。由公式 $CI = (\lambda_{max} - n)/(n-1)$ 得出:CR = CI/RI,其中CR为判断矩阵的随机一致性比率,CI为判断矩阵的一般一致性指标。

RI为判断矩阵的平均随机一致性指标,1~9阶的判断矩阵的RI值参见表4。

表4　判断矩阵的RI值

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.52	0.89	1.12	1.26	1.36	1.41	1.46

当判断矩阵U的CR<0.1,或 $\lambda_{max} = n$,CI=0时,认为P具有满意的一致性,符合一致性检验,否则需调整U中的元素以使其具有满意的一致性。

基于此,可以算出矩阵中的最大特征根 $\lambda_{max} = 4.2262$,CR=0.08471<0.1,说明本文所构建的判断矩阵均能通过一致性检验。

4.4　评估结果分析

根据判断矩阵和一致性检验的分析结果显示,各项指标的权重与实践中所发生的第三方支付信息安全风险事件的原因基本相符合,比较具有借鉴意义。从一级指标来看,平台自身风险、技术系统漏洞所占权重稍大,说明风险集中在第三方支付企业上。政策法规风险所占权重其次,说明国家的法律制度和政府部门的监管应更倾向于信息安全保护方面。用户风险权重偏低,说明此类风险并不受到关注,风险居于最低维度。从第二级指标来看,政策法规的约束力、内部控制风险、纠纷解决机制和权力救济渠道所占权重相对稍大,尤其是纠纷解决机制和权力救济渠道是信息安全风险的重要影响因素,其次是政策法规的约束力较受关注。

对此,如果能对第三方支付信息安全风险进行定期监测,及时采取补救措施,将产生更好的风险防控效益。

5 信息安全风险防范的发展方向

5.1 创新管制思路,明确法律身份和责任

第三方支付信息安全管制未来的发展方向主要是体制机制不断完善,监管思路的不断创新,从而建立健全第三方支付的信息安全法制体系,明确各方的法律身份、权责关系。具体来讲,分为两个方面:其一,从政策法规角度来说,监管机构在已有法规内容不断改进的基础上,应尽快出台第三方支付业务新法规,明晰和规范各方职责范围、权责界定等内容,对违法违规企业或个人进行严肃处理。其二,从非正式支付上看,为确保行业发展的全面性,协会组织的专业性,行业内部可以建立平等的交流合作机制、数据信息共享机制,配合政府相关部门的工作,起到行业内相互监督、督促的积极作用,有效地保护消费者信息安全。同时,随着现代通讯信息技术的日益发达,行业应当借鉴发达国家的先进经验,提高自身技术质量,弥补风险漏洞,尽量减少信息安全风险,更好地为消费者提供支付服务。

5.2 最小化平台运行风险,提高内控管理能力

对于第三方支付平台而言,最小化运行风险、提高平台的实用性是企业长久发展的基础。平台设计初期,企业管理者就应注重平台的整体设计、系统运行的承载能力,聘请专业技术评估人员,对核心业务进行管控及评估,根据业务的发展需求及时调整系统架构,规避系统运行风险。此外,企业应设立紧急事件处理机制,严格按照处置程序,做好应急管理工作,排除平台系统故障,最大限度地减少系统瘫痪风险,缩小停机时间,减轻平台运行风险。

第三方支付企业内部管理能力的提高可从以下两方面进行:一是在监管机构的指导和监督下建立一套完整的内部控制体制机制,包括各项规范、措施,不仅细化每项工作的操作流程、实施监督管理机制,而且对具体操作人员也实行最小化权限原则,严格存储敏感信息,有效规避内部控制风险。二是可以借鉴国际上标准的支付安全评估法则,因地制宜,制定适合本企业发展的支付准则,完善第三方支付行业标准,进而推动整个行业规范发展。

5.3 提高技术手段,强化信息安全管控

第三方支付企业要保障消费者的信息安全,树立良好的信用和形象,必须加大对信息安全技术的投资力度,建立健全第三方支付企业信息安全及监控体制机制,大力推进网络安全认证、风险预警监控和风险评估等先进技术手段的应用,以保障业务的顺利开展。

具体来讲,首先要强化用户身份认证机制,引入电子认证技术,建立可信的网络识别体系并不断验证升级,营造可信的网络交易平台。其次要保障信息储存和传输的安全性,采用自主可控产品,对数据进行加密处理,使数据使用与保管分离,屏蔽网络攻击。此外,使用过滤器,实时监控,一旦发现数据被恶意传输,就会自动阻止,杜绝云端数据泄密。最后,要完善风险防控体系建设,设置防火墙技术,监测软、硬件设施,交易各方建立互信机制,确保业务交易的可靠性,降低信息安全风险。

5.4 完善纠纷解决及救济机制,扩宽救济渠道

2015 年发布的《非银行支付机构网络支付业务管理办法》中规定了第三方支付机构要建立差错争议和纠纷投诉处理等管理制度,按照合理顺序,向用户公告受理流程,并配有专业人员,据实、及时、公正地处理客户投诉,积极接纳用户各项救济诉求。该办法对完善纠纷解决及救济机制有一定的积极作用,客观上推动第三方支付企业认真对待客户投诉,注重自身平台各项服务的完善。另外,我们还应积极扩宽用户的救济渠道,通过协商、和解、调解、仲裁、诉讼等多种方式为投诉客户提供帮助,尽力追回财产等方面的损失,保护人身和财产安全权,维护网络交易的稳定和第三方支付行业的良性发展。

注释:

① 数据来源:国家统计局、中商产业研究院整理。

② 数据来源:瑞星发布的《2018年上半年中国网络安全报告》。

参考文献:

[1] 徐雷, 卓武扬, 李雪玫. 基于网络的移动支付安全风险评估系统设计[J]. 西华大学学报(自然科学版), 2014, 33(6):5-10.

[2] DAN J K, SONG Y I, BRAYNOV S B, et al. A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives[J]. Decision Support Systems, 2005, 40(2):143-165.

[3] 艾瑞咨询.2017年Q2中国第三方支付季度数据发布研究报告[R].2017.

[4] 艾瑞咨询.2017年Q3中国第三方支付季度数据发布研究报告[R].2017.

[5] 艾瑞咨询.2018年中国第三方支付商业职能变革研究报告[R].2018.

[6] 毕建华. 应关注互联网金融信息安全新风险[N]. 金融时报,2016-09-12(007).

[7] 刘杰.互联网金融信息安全风险分析与防范[J].金融科技时代,2015(10):76-77,79.

[8] 冯国震.金融企业中信息安全风险管理[J].电子技术与软件工程,2018(7):211.

[9] 郑志伟.浅谈互联网金融时代背景下的信息安全风险及对策[J].电脑知识与技术,2014,10(13):2953-2954.

[10] 陈哲谦.互联网金融信息安全风险分析与应对[J].科技创新导报,2016,13(15):67-69.

[11] WU Y. The Analysis on the Problems of Third-Party Payment[P]. Management and Service Science (MASS), 2010 International Conference on,2010.

[12] SULLIVAN R J. Controlling security risk and fraud in payment systems[J]. Federal Reserve Bank of Kansas City, Economic Review, 2014, 99(3): 47-78.

[13] 刘春晓.维护第三方网络支付安全加强个人信息保护[J].金融科技时代,2015(12):60-63.

[14] 张鹏.我国第三方支付平台信息安全保障现状分析[J].网络安全技术与应用,2018(9):110,112.

[15] 杨亦军,谭晟.浅谈对第三方支付企业信息安全的监管[J].中国金融电脑,2010(11):79-80.

[16] 毕娟,陈博.基于第三方支付信息安全保护研究[J].纳税,2018(15):202.

[17] 谢迎春.发达国家第三方支付信息安全监管的主要做法及启示[J].财经界(学术版),2017(22):21-22.

[18] 谭超,赵丽霞,张岚.经济新常态下第三方支付企业的内部控制及管理模式[J].财会月刊,2016(5):46-50.

[19] 王思平,李奔.移动支付安全风险及防范措施分析[J].中国市场,2018(29):181-182.

[20] 陈丽莉.基于威胁树的第三方支付信息安全风险评估[J].信息安全与技术,2013,4(8):32-35.

[21] JOSHI M, SINGH V K. Data Security Breach as Perceived Risk and its Influence on Consumer Purchase Decision[J]. Asian Journal of Research in Business Economics and Management, 2017, 7(8): 187-196.

[22] 寿宁静.第三方支付行业中个人信息权保护问题研究——以"支付宝年度账单事件"为引[J].法制与社会,2018(18):68-70.

[23] 周永战,赵颖坤.浅谈第三方支付信息安全等级保护的监管[J].信息网络安全,2013(10):1-3.

[24] 李雪雯.基于层次分析法的电子支付交易风险分析[J].通讯世界,2018(8):233-234.

[25] 危怀安,李松涛.第三方支付信息安全监管影响因素及决策分析[J].统计与决策,2018,34(8):59-63.

[26] 李松涛,危怀安.第三方支付信息安全监管的多元化调查分析[J].统计与决策,2018,34(4):168-171.

Research on the Information Security Risk of Third Party Payment in China

Zhuo Wuyang[1]　Hu Asi[2]　Gong Xingguo[3]　Chen Ting[4]

(1. School of Economics and Management, Shanghai SecondPolytechnic University, Shanghai 200000;

2. XiangchengCounty CPC Office, Xiangchang, Henan 461700;

3. Jining CentralSub Branch of People's Bank of China, Jining, Shandong 272000;

4. School of Economics, Xihua University, Chengdu, Sichuan 610039, China)

Abstract:[**Purpose/Meaning**] While China's third-party payment is developing rapidly, information security risks

are also emerging, which not only causes damage to the rights and interests of all parties to the transaction, but also increases the difficulty of risk management and control. The study of information security risk is helpful to standardize the legal operation of enterprises and protect the legitimate rights and interests of consumers. [**Method/Process**] Based on the former research, this paper analyzes the causes of information security risks, and evaluates the information security risks at different levels by constructing an indicator system. [**Results/Conclusions**] The results show that legal, platform and technical risks have a greater impact on the information security of third – party payments, and relatively lower impact on users' personal security. Therefore, in order to prevent information security risk of third – party payment in China, it is urgent to have innovative control ideas, enhance the internal control management capabilitiesof platforms, improve technology of enterprises, perfect dispute resolution and relief mechanisms, and provide a healthy development environment for third – party payment markets.

Keywords: the third – party payment; information security risk; the third – party payment enterprise; risk analysis; risk assessment

[责任编辑 谭金蓉]

(上接第 5 页)

Study on the Early – warning Mechanism of Natural Disaster Risk Monitoring in Sichuan

Yang Xiaoijie Huang He

(1. School of Emergency Management, Xihua University;
2. School of Management, Xihua University, Chengdu, Sichuan 610039, China)

Abstract: [**Purpose/significance**] Strengthening the construction of early – warning mechanism of natural disaster risk monitoring is an important and effective way to prevent natural disasters and reduce disaster losses. [**Method/process**] This paper investigates the present situation of disaster risk monitoring and early – warning construction, and analyzes the problems existing in disaster risk monitoring and early – warning system in Sichuan Province. [**Result/conclusion**] The paper finds out that the monitoring and early – warning capacity of all kinds of natural disasters have been continuously improved, and the management and coordination mechanism has been updated in Sichuan, but problems still exist, such as incomplete early – warning information system coverage, the low degree of information sharing, the lagging behind of information construction, imperfect information release mechanism, the low awareness of people. Based on this, Sichuan Province needs to strengthen the construction of comprehensive disaster monitoring and early – warning mechanism, coordinate and integrate all kinds of information resources, explore the breakthrough of the "Last Kilometer" early – warning information release technology, and strengthen the publicity and education of all people.

Keywords: natural disasters; monitoring and early warning; early – warning information system

[责任编辑 杨 瑜]