

# Risk and Prevention of Network Payment Industry

Yu Min

School of Finance, Renmin University of China, Beijing  
Email: [13917753252@163.com](mailto:13917753252@163.com)

Received: Jul. 9<sup>th</sup>, 2015; accepted: Jul. 24<sup>th</sup>, 2015; published: Jul. 29<sup>th</sup>, 2015

Copyright © 2015 by author and Hans Publishers Inc.  
This work is licensed under the Creative Commons Attribution International License (CC BY).  
<http://creativecommons.org/licenses/by/4.0/>



Open Access

---

## Abstract

With the development of economy and the progress of technology, China's e-commerce, under the situation of economic globalization, is in the process of rapid development, and online payment services turns from payment tools into a relatively independent industry. However, as for the network system and the computer system and the network payment system itself, there are security risks and security risks, the network payment industry is facing a difficult challenge. This paper expatiates on the related concepts and the development of the network to pay, analyzes the risk of online payment industry, and puts forward China's online payment industry risk prevention strategy.

## Keywords

Network Payment, Electronic Commerce, Risk

---

# 网络支付业的风险及防范

闵 钰

中国人民大学财政金融学院, 北京  
Email: [13917753252@163.com](mailto:13917753252@163.com)

收稿日期: 2015年7月9日; 录用日期: 2015年7月24日; 发布日期: 2015年7月29日

## 摘要

随着经济的发展和技术的进步，我国电子商务在经济全球化的形势下正处于迅猛发展的过程之中，而网络支付服务也从支付工具转变成为一个相对独立的行业。然而，由于网络系统、计算机系统以及网络支付系统自身就存在了安全风险和安全隐患，使得网络支付业面临着艰难的挑战。本文在阐述了网络支付的相关概念和发展情况后，分析了网络支付业风险的表现，并提出我国网络支付业风险防范策略。

## 关键词

网络支付，电子商务，风险

## 1. 网络支付概述

### 1.1. 网络支付的概念

就网络支付这一概念而言，国内外的学者都有着自己的定义。本文中所选用的核心定义是，我国于2010年出台的《非金融机构支付服务管理办法》中第2条规定所描述的：“本办法所称网络支付，是指依托公共网络或专用网络在收付款人之间转移货币资金的行为，包括货币汇兑、互联网支付、移动电话支付、固定电话支付、数字电视支付等。”与传统模式相比较而言，网络支付具有其极其独特的优势。第一点，网络支付是通过数字信息化的手段进行的，以信息传递的方式来达到交易支付这一核心目的，基于此，对于网络安全也有着极高的要求；第二点，网络支付中将会涉及到消费者、商家以及第三方平台等多个交易相关群体，与传统模式相比更为复杂多变；第三点，网络支付所具有的最大优势就是快捷高效，交易双方只需使用终端设备接入网络，简单操作之后就可以完成交易；最后一点，网络支付以互联网为通信方式，这对于软硬件都有一个较高的要求[1]。

### 1.2. 网络支付在我国的发展

无论在地球的哪一端，网络支付平台是一个刚刚开始蓬勃发展的新兴事业，随着网上支付的广泛普及，业已产生了对社会的巨大且极其深入的改变，正在彻底的改变着我们的生活模式。网络支付涉及到资金安全的问题，并与社会的稳定有着密切的关系。国内目前已经有了三百余家企业拥有了网上支付的业务。以所提供的服务形式进行分类，可以将之划分为两大类：其一是账户模式，用户在平台之上设立自己的账户，向平台账户中进行充值，并用平台上的账户资金进行支付活动；其二，网关模式，为用户提供各银行支付平台与接口衔接上的统一支付渠道。

在电子商务的业务范围内，主要是以下四个方面的内容，即信息流、商流、资金流、物流。资金流的核心内容是资金的转移过程，即支付、转账等交易流程，而支付和转账等交易流程都是以网上支付的形式进行的。追根溯源，网上支付是电子商务中的一个重要组成内容，没有现代化的支付手段，电子商务将面临极大的困难。目前，国内银行业的主要收入源是存贷之间所产生的利差，故而，尚无暇染指网上支付这一新兴领域。还有一个麻烦之处是，电商企业所拥有的客户可能同时与各银行的客户是同一个群体，如果与银行一一进行谈判并逐一进行技术后台的调整，成本将非常之高。因此，第三方平台的出现占领了这一商机，在资金流转之中充当了至关重要的角色[2]。

我国的电商产业正处于一个高速发展的阶段，网上支付服务已经从过去的支付工具逐渐转变成了在今天来说一个比较独立的行业。在这一现实基础上，我国已经出台了相关的政策法规对网上支付行业及

时的实施监管，提升行业内的规范，加大非金融机构的准入门槛等有效措施。这对于预防支付市场所可能存在的风险，保护金融安全、维护用户权益有着极其积极意义。

网上支付中所存在的问题一直制约着我国的电子商务发展，网上支付平台近年来的长足发展已经有效的缓解了问题。《电子签名法》已经在发挥自己的效力，《电子支付指引》也已经正式颁布，这都大大起到了规范电子商务网上支付环境的作用，良好的电子商务支付环境正在日益完善。2011年，选择网上支付进行交易的比例已经高达72%，一多半的网购者开始青睐于网上支付这一交易手段。这同承担着中立第三方角色的网上支付平台的出现和日渐完善是密不可分的。支付平台使得交易款项的交割更加便利性，其功能也具有着较大的可拓展性，最重要的是作为第三方提供了自己的信用保证，这就极大解决了长期影响着电商行业发展的诚信、物流、现金流方面所存在的问题。支付平台的出现是对交易双方的权益的最大维护，使得无论是中小企业还是个人用户，都可以有安全感的进行网上交易。更安全、诚信的网络消费环境是势必要要在未来逐步形成的[3]。

国内，网络支付最为主要的方式是使用银行卡进行交易。根据CNNIC在2014年进行的报告，汇款、网络支付和货到付款三种支付方式分别占到了总交易数的43.1%，41.9%和34.7%。过去的调查中显示，网络购物交易中的支付方式使用银行卡进行网络支付的比例逐年呈递增趋势，已经由2001年底的15.6%提高到了2014年6月的46.9%。由于利润问题的存在，银行卡进行支付的问题尚未根本解决，基于此，现金流仍将是网络购物之中存在的重大问题之一。与此同时，网络支付的安全性仍然没有得到真正的认可。42.3%因为怀疑网络购物的安全性而没有选择网络支付手段。在网上进行采购的产品，主要集中在500元以下的商品之中，年龄主要集中于18~30岁这个相对年轻的群体之中。目前，人们仍然只是把网上购物作为一种新奇的事务，多数采取保守态度，网上购物并未成为他们的主要购物方式，就贵重的物品的购买而言，出于安全考虑，很少会在在网上进行购买。

网络支付中还存在着另一个令人担忧的安全因素，即信用与身份识别问题，有相当大比例的人对信用与身份识别问题心存疑虑。消费者所担心的最为主要的问题仍然是网络购物中产品的质量。

## 2. 网络支付业的风险的表现

### 2.1. 系统风险

系统风险所指的是银行网络支付系统所存在的安全漏洞或不足，所可能引发的损失。网络支付是依赖于网络环境而得以完成的，故而，信息系统之中，在技术或者管理上所出现的问题，将会构成严重的系统风险。当系统同交易方进行信息传输时，若系统与交易方的终端不兼容或出现故障，则会出现传输中断或速度降低的问题。除此以外，若是电脑死机、磁盘破坏、病毒侵入等问题，都会产生系统风险。在未来大部分的交易支付都将会依赖于网络进行，因系统本身局限性而存在的风险，势必将会妨碍到网络支付的顺利进行。2004年时曾出现了一个称为“网银大盗”的木马，其轻易突破了银行系统，并窃取了用户的账号、密码，这极大的妨碍了网络支付的顺利发展[4]。

### 2.2. 人为风险

人为风险所指的是在交易之中，个人因素所导致的密码及其他重要信息的泄露所产生的风险。大多数金融机构基于成本考虑，会寻求外部力量的帮助来解决营运中的技术或管理问题。这是一种双刃剑的做法，解决自身问题的同时也将自己暴露在于风险之中。

#### 1) 金融机构外部风险

黑客通常会采用IP地址欺骗、篡改用户数据等等的技术来达到自己非法牟利的目的。黑客会将自己伪装成某一受到信任的主机，向其他主机发送含有病毒的信息包，或是在邮件服务器中冒名他人信息。

较为常见的黑客侵袭方法还有拒绝服务攻击、同步攻击、网页欺骗等等。手段多样，且不断翻新，让人防不胜防。

一些电脑高手所设计的病毒与木马是网络支付安全之中的一个巨大威胁。各大网站甚至一些知名网站也难以幸免的被安放有后门。这些黑客程序不仅会破坏电脑系统，还会盗取当事人的账户信息等敏感内容文件，对人们网上支付造成了极大的危害。美国的银行账户，每年在网络上损失的总金额高达 6000 万美元，与此同时企图进行的电子盗窃案的总数更是到达了 5~100 亿美元，持械劫匪抢银行的平均作案值能达到 1500 美元，“电子扒手”的平均作案值则能够达到 25 万美元[5]。

#### 2) 金融机构内部风险

对于网络支付行业的从业人员方面的管理，是网络支付安全之中相对薄弱的一环，这一群体具体掌握着网络支付流程之中的各环节，网络认证、防火墙等方面的工作都是由这些从业人员来完成的。目前国内的网络支付案件不少是由于内部人员所引起的，有逐步上升的一个趋势。网络支付的安全保护系统被从业人员自内部“攻破”之后，无论是多么先进的技术手段也都无能为力[6]。

### 2.3. 信用风险

信用风险又被称之为违约风险，所指的是网上支付中各交易方无法或未能履行约定义务而造成经济损失的风险。

#### 1) 买方失信

买方违约的情况。以资金角度出发，虽然买方不履约，未必会造成卖方或第三方企业的资金损失。不过，这样会增大支付企业的营运成本和信用成本，低信用度用户的比重将增大，各类风险都会有所增加。买方所存在的信用风险还可能会涉及到资金来源是否合法、买方否认交易操作、以虚假身分进行交易、洗钱等等问题。

#### 2) 卖方失信

卖方提供不出与买家商定的产品，不能以预定时间送达到客户手中，这将会引起买方的相关损失，如退货的相关费用、与卖方交涉所产生的时间成本及其他费用，卖方自身的运营成本和诚信成本大幅增加，造成信誉的极大损失。

#### 3) 银行失信

银行在迟延结算或是非本行银行卡交易时发生拒付，迟延结算等问题将会产生资金流动性风险。网上银行以远程通信为方法，经由信用认证相关程序对借款者的信用进行自己的风险评估，这可能会增加网上银行自身的信用风险。借款人未必会履行电子货币的借贷所应当承担的义务，也可能由于借贷人评估系统不够健全，进而造成信用评估产生失误，引起银行的误判。

### 2.4. 运营风险

从银行角度出发，此类风险所指主要是交易的处理、流程管理中的失误或者是与贸易伙伴之间关系的破裂而造成的损失，产品在特性或设计上存在不合理之处、员工服务漫不经心，亦或者是对特定客户不能提供应有的专业服务而产生客户流失等原因而引起的银行损失。业务账目记录错误、信息交流之中存在错误信息、没批准而擅自账户录入、未得到客户允许就进行的交易、交割过程中产生的失误等原因所产生的各类损失，产品自身的功能欠缺、强行进行销售、对敏感问题的隐而不发、不当的客户建议、职员操作过程中的粗心、广告内容缺乏合理性、交易的不合理性、销售过程中的歧视态度等等问题，导致与客户之间的一个信托关系发生破裂、合同关系发生破裂、客户关系发生破裂，进而造成的各类重大损失[7]。

### 3. 我国网络支付业风险防范策略

#### 3.1. 完善网络操作系统

在网络通讯以及相关的应用系统之中必须要大量应用具有较高安全性的相关加密设备。防火墙、身份认证技术以及各类信息加密技术等是必不可缺的设施。特别是银行系统，更是需要使用多种类型的加密设备，如加密机以及支付密码器和卫星通信保密设备等等加密方式对所经手的信息进行严格的加密，进而实现跨地域、跨银行、跨币种的平台兼容性。安全保密技术以及设备的有效应用，大大提高了网络数据在传输过程中的安全系数，可以有效的防止资金被盗，网上银行通过对这些保密技术的有效使用，也可以更好的保障自身资金的一个安全。在系统设计这一概念上，已然舍弃了先前简易的一种单向认证方式，进一步的完善了客户信息处理系统，并更深入的建立了客户身份证件电子文件信息库，有效实现了各系统之间内部的信息共享。这样就可以在需要调阅相关客户信息的时候，可以对客户提交的信息进行审核，核对前后信息是否一致，并核查其真实性。这样可以有效的减少不法分子的欺诈行为，减少网络支付环境中的危险[8]。

#### 3.2. 降低网络支付人为风险

降低网络支付中所存在的人为风险，从加强培训方面切入，是可以有效解决这一问题的，提高柜员自身的识别力，可以有效的降低这一风险。

对身份认证进行强化，是有效防范网络支付中的风险里，最为直接的一个手段。强化系统设计上的认证方式之外，在柜台进行的具体流程的操作也是至关重要的一个环节。要对利用伪造信息进行冒名注册的行为进行防堵，同时，如果能够及时识破假造的银行账户凭证，可以有效降低支付过程中的风险。基于此，进行相关的强化培训，可以有效提高柜员自身的一个防范的意识与识别的能力；除此之外，也要为柜员创造一个有利的条件，当拥有一套完善的客户信息库，并能够建立完善的客户身份信息电子文件库，在系统内实现信息的及时有效的共享，在如此便利的一个条件之下，柜员将可以更方便的识别出伪造的虚假信息。这就可以更有力的堵截非法分子的不良企图[9]。

#### 3.3. 完善社会信用体系

##### 1) 严惩不守信用的违法企业

第一，要严格实施市场退出这一制度。相关的政府部门，应当要建立一个就从事信用服务企业而言行之有效的惩戒机制。一定要明确规范行业规则，有效提高行业内自身的一个自律能力。对于那些背离行业操守、拒不守信的企业，就一定要让其承担相应的责任，甚至于是永远的让其退出这一行业，决不能任其肆意的扰乱整个信用市场。

第二，应当明确拥有对失信企业进行有力惩戒的政府部门究竟是哪一个部门。这里可以向美国的相关政策进行学习，其在对失信行为惩戒的政府相关部门划分成了两大类，其一是金融系统方面的管理部门，如中国人民银行证监会；其二是非金融系统的方面的管理部门，如国家经贸委、国家工商总局、国家质监局。在此基础上，细化权责，明确细节，可以在有效的保证惩戒力的同时，避免管理区的重合所产生的责任扩散。

第三，建立相关的司法处理途径。将社区义务劳动与社区矫正和罚款有机结合在一起，甚至是有期徒刑等各类短期刑罚综合实施，迫使失信的相关人员承担起自己应当要承担的责任，使其付出相应的代价，提高失信成本，这将能够有力的降低相关者背信弃约。

##### 2) 实行信息公开和共享

在虚拟空间之中所进行的贸易活动，发生相关的支付行为，交易双方本身的一个信用度对资金安全

有着至关重要的意义，建立一个在全国范围内可以有效共享的信用数据库是极其有必要的。政府相关主管部门有必要大力推动银行信用卡这一制度，并由银行，以信用卡使用情况为基础信用信息。并将整合政府各部门现今已经收集到个人相关信用信息进行整合，建立健全一个全国范围内的信用信息数据库。此外，第三方机构和消费者也要参与进来，完善企业与个人的信用信息，进一步的完善这一信用信息库的建立完善[10]。

### 3) 强化身份认证，废弃简易交易

过于简单的身份认证信息以及过度简单的账号密码都导致了网络中的信息泄漏和资金的被盗。若是想要从最本质上降低网络支付自身的一个风险，强化身份认证是势在必行的一大措施，并配合以强制性的提高注册要求，限制信用等级和其可信度来保证信息的真实性。舍弃只是采用简单的账号密码这种过分简陋的传统认证方式已经到了不得不改变的时候了。在进行任何网上交易行为之前，必须要事先通过柜台进行详细的申请注册，成为网上银行的认证用户之后才能进行，并辅助以经第三方权威机构进行相关的核实之后提供的数字证书作为支付的一个重要认证内容。有关的监管部门也必须要明令禁止商业银行为只是基于账号加密码认证方式之下所进行的查询和转账这两种服务。

## 3.4. 加强对网络支付第三方机构的监管

### 1) 建立第三方支付平台的准入机制

国内目前的法律法规仍然缺乏相应的关于第三方支付平台准入机制方面的条款。相关的立法部门应当要为第三方支付平台企业顺利合法的进入该领域制定一个行之有效的市场准入制度，对其进入的标准设立具体的条件限制，于此同时，必须要限定只有国家机关才有审批通过中介服务准入资质的权利，而不能放权。尽快地建立健全第三方支付平台的一个市场准入机制，是有效保障第三方平台自身的经营主体资格的最佳途径[11]。

### 2) 制定相应的第三方支付退出保障机制

第三方支付机构所涉及到的客户数量是极大的，且客户的分散性也是极强的，故而，当第三方支付网络支付机构要退出市场之时，必须要有一个完善的保障机制，严格确保其退出这一行为不会损害到客户权益。这里要主要关注以下两点：

#### ① 确定合理的备付金退还方案

第三方机构解散之后，所产生的最直接的一个问题就是，客户已经支付到平台上但尚未消费的资金如何进行处理。在笔者看来，第三方机构应当要制定多种可行方案以备客户进行选择，还可以向网上银行的退出方式进行学习，可以对客户的资金进行再次保险，在解散后的退还过程之中对客户资金实施严格的管理和核查程序，要认真确保客户能够在最大限度之上获得自身资金的返还。

#### ② 制定客户权益保障方案和业务信息处理方案

《非金融机构支付服务管理办法》进行了相关的规定，第三方机构首先应当要对自身的业务终止缘由和手续流程等事宜进行详细的通告，要对客户隐私信息所进行的处理进行详细的说明，要保证客户的隐私信息不被泄露。

## 3.5. 加快网络支付相关法律法规建设

### 1) 完善现行法律应对多变的计算机病毒与木马犯罪

当今的科技发展速度之快，令人叹为观止，在网络中伺机作案的计算机病毒犯罪态势也成一个日趋严峻的走向，政府有关部门必须要尽快制定行之有效的法律法规予以打击，建立健全一些相关机构以应对相关问题。

配合《计算机信息网络国际联网安全保护管理办法》当中规定，细化关于网络犯罪的具体定义，以及惩戒方法。只有适当的惩戒才能防微杜渐，阻止网络犯罪的大肆猖狂，使之得到应有的惩罚。

## 2) 完善网络支付的相关法律法规

第一点，建立健全完善的电子支付相关的法律法规是极其有必要的，首先应当要统一整个网络支付的标准和规范。向国外的先进经验学习是必不可少的过程，此外，也要积极的将国外的先进知识同国内的具体情况相结合，进而制定符合于我国国情的自成一体的一统网上支付标准和规范。这样就能够大大减少支付标准不统一所可能带来的风险，也可以大大便利消费者。

第二点，有关部门应当要加强对电子支付方面的法律法规进行有力的执行监督，协同银监会、证监会、保监会三者共同进行监管。对电子支付的相关网络金融业务等，建立三方联席会议制度，协同监督管理，进行及时的信息资源共享，并及时通告各自的实时监管情况，协同合作密切配合，共同进行防范网络风险犯罪。

第三点，最后一点，也是极其重要的一点。我们应当要加强金融监管的国际间合作。网络安全与经济安全，社会安全同国家安全之间是紧密联系，密不可分的，为了能够有效防范网络风险所可能引发的金融动荡，世界各国之间应当要加强多方的协同合作，这样才能在当前这个世界一体化的情况之下最大限度的保障国家和世界范围内的金融安全。

## 4. 结语

新兴的电子商务是同网上在线支付密切相关的，电商这一现今互联网络之中至关重要的一项商业活动，是现如今信息与网络大盛的时代背景之下的必然产物，依托于现代化的信息技术与网络技术的有机结合，并进一步融合了金融电子化、管理信息化，实现物流、资金流与信息流三者之间的和谐统一的新型贸易方式，这一贸易方式将可能成为 21 世纪经济发展之中的一个极其重要的推动力。正因为如此，世界各国政府都纷纷加快了本国电商的发展速度，想要抓住这个具有空前历史性的发展良机。网络支付，是在科技、经济都飞速发展的这一时代大背景之下所孕育而产生的，传统的支付方式已然不能再满足人们在新时代支付需求，各个支付机构都悄然在各自领域之内努力孕育着自己的新力量，经由市场的检验而创立健全了崭新的支付方式。

## 参考文献 (References)

- [1] 阿拉木斯 (2007) 第三方网络支付平台所面临的七大法律风险. *电子商务*, 1.
- [2] 阿拉木斯, 主编 (2006) 网络交易法律实务. 法律出版社, 北京.
- [3] 敖东梅 (2008) 略论中国电子商务立法的现状及其完善. *商场现代化*, 4, 262.
- [4] 曹小青 (2005) 网络支付的安全与标准统一. *中国计算机报*, 12.12.
- [5] 陈雷 (2007) 国外电子支付的消费者保护. *软件世界*, Z1, 81-82.
- [6] 陈建平 (2005) 试论政府角色定位之理论范式的变迁及启示. *云南行政学院学报*, 5, 45-47.
- [7] 陈文玲 (2003) 中美信用制度建设的比较和建议. *南京经济学院学报*, 2.
- [8] 徐学慧 (2008) 第三方网络支付的现状与发展. 北京邮电大学, 北京.
- [9] 赵公民 (2007) 我国网络支付平台下买卖双方利益保护机制研究. *中国流通经济*, 9, 32-34.
- [10] 黄卓君, 朱克武 (2007) 网络支付风险及其防范. *农村金融研究*, 3, 57-58.
- [11] 谭彬, 薛质, 王轶骏 (2007) 网络支付体系的安全性分析与研究. *信息安全与通信保密*, 11, 61-62, 65.