第 8 章　网络支付的法规和监管

教学目标

通过本章学习，了解网络支付环境中存在的各种风险，认识法规与监管对确保网络支付健康发展的必要性，熟悉国内外在网络支付的法规制定与监管方面的实践、取得的成效和尚待解决的问题，探讨在未来如何加强网络支付环境的法律规范化建设。

教学要求

知识要点	能力要求	相关知识
电子货币的法规监管	(1) 掌握电子货币的属性，与传统货币的差异性 (2) 电子货币发行的要求 (3) 现今电子货币监管实践	(1) 电子货币的法律属性 (2) 电子货币的发行过程 (3) 电子货币的立法
电子支付的法规与监管	(1) 国内外有关电子支付的立法知识 (2) 网络支付中存在的各种法律关系 (3) 电子支付的监管	(1) 国内外有关电子支付的立法 (2) 网络支付的法律关系 (3) 电子支付的监管措施
网络银行的法规与监管	(1) 网络银行相关国际法律法规现状 (2) 网络银行的法律风险 (3) 如何防范法律风险 (4) 网络银行的监管	(1) 网络银行相关国际法律法规 (2) 电子支付指引 (3) 法律风险的防范措施 (4) 国内外网络银行的监管实践
第三方支付的法规与监管	(1) 第三方支付中的法律关系以及潜在的问题和风险 (2) 我国现有第三方支付的监管情况及监管趋势	(1) 第三方支付中的法律关系 (2) 第三方支付的潜在问题和风险 (3) 现有第三方支付的监管情况 (4) 我国第三方支付监管现状及监管趋势
第三方认证中心的法规与监管	(1) 电子认证中的法律关系责任 (2) 我国第三方认证相关立法 (3) 如何设立、终止及监管认证中心	(1) 电子认证中的法律关系分析 (2) 电子认证中心的法律责任 (3) 我国第三方认证相关立法 (4) 认证中心的设立、终止及监管

导入案例

支付体系发展，安全先行

2007 年 9 月中国人民银行支付结算司司长许罗德在全国地方金融第十次论坛会议上表示，“近年来，我国支付体系建设在 4 个方面可以说获得了突破性进展，特别是在支付系统建设方面。”支付体系包括支付系统、支付工具、支付服务组织、监管法规与机制 4 个方面。“异地汇款零库存优化了备付体系，支付系统上马后，大型银行的备付金率下降了 0.5 个百分点。”许罗德强调，主动划汇、个性化付费等公共支付平台在为居民提供便利的同时，也为银行创新支付产品创造了更多机会。

但在看到支付体系建设取得突破性进展的同时，人们也意识到由于支付体系所依赖的开放网络的硬伤，使得支付体系以及网络支付在实施过程中遇到众多的问题。在 2008 年 10 月 13 日，不少消费者向 315 消费电子投诉网站投诉网银被盗现象，而被盗账户资金从几百元到几千元不等。2008 年 9 月 3 日下午，董先生用工商银行网上银行交电话费时，发现银行卡里的钱都没有了。董先生立即去查询账单，发现 8 月 29 日下午，账户向上海环讯电子商务有限公司这个户口打了 440 块钱。“我也从未在网上购物，账单上也没有注明买什么东西。这笔钱为什么会到了这个户头？”对此，银行也无法解释。

董先生的遭遇并非个案。据 315 消费电子投诉网介绍，当时，全国就有 57 位消费者投诉反映，网上银行、信用卡的账户莫名其妙被盗，而其中有 11 个账户被盗后，资金都汇款到一个第三方支付平台——上海环迅电子商务有限公司的账户。当消费者要求该公司冻结账户资金时，却遭到公司的敷衍和拒绝。上海环迅电子商务有限公司风险控制科杨先生表示，作为一个电子商务第三方支付平台，买家将资金打到该公司账户后 3 天内，公司就要把资金汇给卖家，而资金一旦汇出，就不可能追回。“我们无权冻结资金，也没有技术认定账户是不是被盗用，当客户怀疑账户被盗时，我们只有协助公安机关，提供账户交易记录，调查被盗情况。”

在目前的情况下，无论是银行还是第三方支付平台，一项新产品推出，一项新技术的应用，都是在不断地进行实验，然后发现问题，进行产品的升级与改进，一位资深的银行主管曾说，“我们也是不断地在和科技犯罪分子打交道，所以很多产品在当今日新月异的技术变化中，或多或少都存在着一定的漏洞。”而当出现问题时，例如案例中董先生的网上银行账户被盗，资金损失时，通常无论是银行还是第三方支付平台，其说辞都是只能协助储户进行调查，并不一定能将被转走的钱找回来。因为很多情况下银行和第三方支付平台在遇到这些突发情况时，并没有相关的法律作为依据对事件进行处理。目前，我国对支付行业的监管还停留在传统银行监管方式上，法规不明确，支付责任界定模糊，网络支付问题一旦发生，解决起来就十分困难，而且，目前的发展状况也表明，监管缺席已经导致网络支付产业链各个主体之间缺乏系统的权责安排。另外，无论是银行还是第三方支付平台，其凭借着自身的优势，使得储户在遭受损失之后跟银行进行沟通解决时，银行或者是第三方支付平台通常扮演着一个强势的角色，因此为了更合理的保障储户的合法权益，促进银行(或支付平台)与储户平衡相处，促进网络支付市场的合理发展，制定相应法规的要求已经十分迫切。

资料来源：http://www.lodoeshop.com/news/ld_news2540.html.

问题：

1. 网络支付系统发展的同时给我们带来了哪些问题？
2. 根据你的了解，谈谈我国现今网络支付法规和监管现状？

从导入案例中看出，网络支付在我国获得了空前的进展，丰富了现有的支付体系，给人

们提供了更多的支付选择，从长远来看，还将有巨大发展前景。然而，在网络支付进步的同时，也带来了一系列问题，它们是网络支付(区别于传统银行)独有的问题，如何解决好这些问题，关系到网络支付的长足发展，这需要网络支付运营者和监管机构的共同努力。

8.1 电子货币的法规和监管

网络支付系统的突破性进展为支付系统注入了一份新的活力，增强了现有支付系统的功能，给人们提供了更多的支付途径。正如传统支付系统依附于纸币等传统货币，网络支付系统是建立在电子货币基础之上的。电子货币的应运而生是新世纪以来网络经济不断推进与繁荣的结果，它的出现大大方便了广大的网络消费者，它完全跃出了传统的商务活动中的资金划拨，它的便捷性完全符合和支持了电子商务中资金流的运作。电子货币已经成为了发展电子商务的核心部分。电子货币的普及和应用都将为网络经济的发展开辟新的、更为广阔的天地，使之在服务领域产生更大的效益。然而，随着电子货币的出现也带来了一系列的问题，在实际的试运营中已凸现出了电子货币这一新的支付手段跃出传统商务所采用的支付方式与手段的法律规范框架的矛盾。解决所出现的问题及化解这些矛盾，首先要确定电子货币的法律属性以及在法律上如何去规范电子货币的问题。这些问题的解决，都将为电子货币的普及扫清法律的障碍，奠定规范的运作基础。

8.1.1 电子货币的法律属性

由于立法实践的滞后性，在法律上至今还未有对电子货币这一新出现的支付手段作出一个明确的定义和划分。在对电子货币的法律属性的了解和认识上，不同领域和群体持有不同的观点：有人认为电子货币是传统货币的辅助支付表现形式；也有人认为电子货币是完全脱离传统现金货币的支付方式，甚至可以完全替代传统货币等等。不同的看法体现了电子货币在立法中的法律地位的不确定性。如何客观地解决这个问题、认清电子货币的法律属性涉及了整个电子货币的全面立法规范问题。客观地看，可以从以下几个方面来分析、探讨电子货币的法律属性问题。

1. 电子货币的流通与使用角度

电子货币作为支付手段，在各国早已被提到快速发展的日程上来，有的国家在某些领域或局部商务往来中已经进行了电子货币的试运营操作。虽然，在各国的法律中还没有明确规定或指出电子货币的货币法律性，然而从现实的发展趋势上分析，包括我国在内的很多国家，在现实的金融运作中已经默许了电子货币作为支付手段的存在，实际上也是肯定了电子货币作为一类货币形式的存在。立法是在社会实践的基础上，进一步地确立其法律地位，完善、规范其运作模式。因此在实际实践中的普遍推广与应用，更会为电子货币的立法工作积累丰富经验，促进、加快电子货币的法律规范建立的步伐。

2. 电子货币与传统货币的关系和比较

电子货币是完全依赖于电子化的高新技术，它是一组虚拟的模拟数据，并以互联网技

术为操作平台，支持其发行、流通和回收的整个过程。从是否使用介质上分析，电子货币与传统的货币有着本质的区别和不同。电子货币可以以一种存储货币数据的载体为介质，如信用卡、IC 卡等。但也可以完全虚拟化、数据化，不需要介质。而传统的现金货币，是以金属或纸张作为介质的。此外，从货币的流通上看，也就是从商务交易中的资金划拨中分析，电子货币还不能直接由交易双方来进行操作，因为它涉及发行实体，即电子货币的发行银行或金融信用机构，以及第三方的银行和认证体系。在交易中必须有发行电子货币的金融实体及认证系统，对客户进行身份确认。在交易过程中，彼此间真正的资金划拨是在电子货币的发行机构与接收方的开户银行间幕后完成的，也就是说，商务贸易双方只是直接接触者，而真正的划拨资金是在后方完成的。而传统的货币资金则不同，它是以贸易的双方直接进行货币现金的实体交易与结算的，也就是一次结算、当场结算。其中只有极少数的大额资金在银行间转账类似于电子货币交易的过程，属于二次结算。

虽然如今电子货币有了很大的发展，但从某种程度上讲它是不可能完全取代传统的现金货币的，因为它没有传统货币那样作为本国法币的法律地位和效力。法币就是法定货币，是法律明确规定的用作商品交易的货币。就物质的价值而论，传统的现金货币，在具有使用价值的同时，其本身也具有所属的价值性，与一般流通货币相比较，它的价值主要体现在它作为法币的不可动摇的主导地位。然而，电子货币作为支付的方式、手段，由于它本身的数字性等特点制约，它仅主要体现了其使用价值，而其价值性却显得非常薄弱，这是电子货币与传统现金货币的一大本质区别。因此，目前电子货币只能作为广义上的流通货币出现，只是一种新形式的支付手段。

由此可以分析出，电子货币虽然在很多方面与传统的现金货币有着区别，但是它们并不相互排斥，是可以同时并行存在的。从现实的使用中以及电子货币的虚拟、数据化和便捷等特点可知，它已经成为了一种以现金存款货币(法币)为基础的、并使之信息化的二次性货币，它们的本质是一样的，不同的只是形式改变，它是传统货币的升级而又不脱离传统货币，它们有内在的必然联系。

8.1.2 电子货币所引发的法律问题

电子货币的产生和发展，对原有的市场交易法律体系和框架构成了挑战，主要表现在以下几个方面。

1. 电子货币的发行主体难以确定

我国目前并没有关于电子货币的专门立法，仅仅在 l999 年颁布的《银行卡业务管理办法》及 2004 年颁布的《电子签名法》中对电子货币有所涉及。《银行卡业务管理办法》规定了储值卡属于银行卡，却没有明确规定非银行是否可以发行储值卡。《电子签名法》主要是规定了电子签名及其认证，为电子签名技术应用于电子货币提供了法律保障，却没有涉及电子货币概念、电子货币发行主体等相关问题。发行主体发行电子货币的目的在于获取利益，这些利益一方面来源于发行电子货币所收取的费用，另一方面来自于发行主体将所获资金用于贷款或投资所得利润。为了追逐利益，很多机构都想发行电子货币。但是，究竟谁可以发行电子货币，在法律上没有明确规定，发行主体的不确定性极易造成对电子货币监管的失控。电子货币的发行作为电子货币法律问题的重要组成部分，将在“8.1.3 电

子货币的发行”一节中重点介绍。

2. 电子货币相关方发生纠纷的责任难以确定

电子货币从根本上改变了传统的支付方法，通过电子货币赖以生存的计算机网络系统，能在瞬间内完成资金的支付和划拨。资金划拨所涉及的当事人很多，除了顾客本人、网上银行等发行主体外，还包括资金划拨系统经营主体、通信线路提供者、计算机制造商或软件开发商等众多的相关方。当出现某种故障无法准确的进行资金划拨时，很难确定各方所应承担的法律责任。

3. 电子货币隐私权难以保护

一方面，电子货币的发行主体通常也发行私人和公共密钥、从事密钥的管理，而密钥事关客户的个人数据隐私，这些资料一旦公布，对客户将造成较大的影响。其次不排除电子货币发行主体向第三者出售这些数据资料牟利的可能性。如有一方发行主体保存着电子货币使用者的交易记录及其他基本信息，如果将这些合法收集的资料用于所声明的目的以外的事项，对当事人将造成重大损失，交易当事人的隐私权保护就无从谈起。可见，电子货币有可能带来客户的隐私权保护问题。

4. 电子货币的安全难以控制

首先是安全认证的标准不统一。我国已有的网上银行所采用的安全认证方式各不相同，国家也没有一个明确的标准，对电子货币安全技术系统的认定没有相配套的法律约束和保障。其次是虚拟交易安全性下降。电子货币将以前孤立的系统环境转变成开放的充满风险的环境，电子货币产品也增加了一些诸如鉴定、认可、完整性方面的问题，安全风险可能在消费者、商家或发行者任何一个层次上发生。

5. 电子货币带来洗钱难题

法律上对传统洗钱方式进行控制的重点在银行，主要是通过银行对交易的记录和调查来预防和发现洗钱犯罪活动。因为，在电子货币出现以前，洗钱犯罪活动是以银行为中介进行的，银行具有控制客户活动的能力，而洗钱活动是利用了有形货币。然而电子货币的出现则对反洗钱提出了挑战，电子货币的匿名使得了解客户更加困难。随着越来越多的非银行机构成为电子货币的发行主体，电子货币使得交易各方直接进行电子交易，这就造成洗钱活动不会留下传统上的犯罪证据，给反洗钱的执法机构带来了难以逾越的障碍，阅读案例 8-1 中，犯罪分子就是利用了网络银行和网上的外汇买卖，进行诈骗犯罪活动，并历时一年多才被侦破。

阅读案例 8-1

网上银行暴露巨大漏洞

在深圳布吉关口，涉嫌一年前伙同他人在深圳和茂名两地洗钱 28 亿元的嫌犯张某被抓，至此这起大型洗钱案潜逃的 3 位嫌犯悉数归案。

该团伙成立大量空壳公司，控制数百个个人账户作为过渡账户，大肆进行非法经营、洗钱活动。通过网上银行转账和外汇买卖操作，进行境外境内收支两条线的跨境运作。

张某提供的自白书显示，2007 年其在深圳为电话充值卡经销商打工，经常会出入银行办理业务，有一次他需要从对公账户上取现，被银行工作人员拒绝，要求其在银行开立基本账户，开通网上银行后，公司转账汇款可以在网上银行自己办理，可以代发工资，并能将对公账户上的现金转到个人账户。他发现这里存在玄机，操作过程中可以获得利润。

但张某苦于没有本钱和客户，当经销商陈裕潮采购充值卡时，他向陈道出生财之道，两人一拍即合，并说好利润五五分成。去年 3 月份，张某到茂名开设基本账户，后又在深圳开设，利用网上银行代发工资的业务，将对公账户的现金转到个人账户。去年 4 月份开始，几人开始疯狂开设数百个账户转账，转账 10 万元可以得到 20 元到 50 元不等的利润，直到 2008 年 6 月 3 日公司账户被冻结。

资料来源：http://www.chinaz.com/News/hearsay/052CHb2009.html.

问题：

1. 上例中的犯罪人利用了网络银行的什么漏洞来进行洗钱？
2. 通过上例，你认为银行应采取什么措施来避免这种漏洞？

阅读案例 8-1 中，罪犯利用网络银行代发工资来进行谋利，涉案金额达到几十亿后才被发现，说明银行在洞察网银业务的犯罪活动方面存在严重滞后性。因此，银行在开展网络银行业务的同时，应该加强犯罪预警机制，及时发现漏洞，完善网络银行业务。

6. 通过银行卡进行网络支付所产生的法律问题

银行卡是银行或其他金融机构发给消费者的用以存取现金、在约定单位购买商品或支付劳务、定期结算清偿的金融工具。目前有很多关于银行卡流通的法律规定，涉及发卡、授权、结算、挂失等许多环节，涉及各个当事人之间的权利和义务关系。其中最为核心的问题是未经用户授权使用银行卡所造成的损失如何由商家、消费者和发卡银行分担。这种损失分担的机制直接影响到各个当事人使用银行卡的积极性，以银行卡为基础的网络支付体系也必须考虑这种损失的分担问题。此外，由于通过开放的互联网络传送有关的银行卡信息，采取哪些手段保护这些信息不被非法利用也是一个新的法律问题。

7. 数字现金流通中产生的法律问题

数字现金是以电子化数字形式存在、流通的货币，是由 0 和 1 排列组合成的通过电路在网络上传递的信息电子流。数字现金通过因特网上的电子邮件或任何其他的计算机网络系统，在线进行交易和支付。数字现金的使用会产生许多法律问题，如数字现金的标准与使用安全问题；保护使用数字现金的消费者利益的问题；防止通过利用私人网络进行洗钱和防止伪造数字现金的问题等。

8. 电子支票使用中产生的法律问题

电子支票是一种用数字化手段将纸质支票改变为带有数字签名的报文，利用数字传递将钱款从一个账户转移到另一个账户的电子付款形式。电子支票使用数字签名技术，电子支票中最大的问题就是数字签名在票据法上的效力问题。在票据法中有必要承认数字签名的合法性，也可以通过制定一些新的法律法规来调整电子支票的流通。

8.1.3 电子货币的发行

1. 电子货币发行主体的权限

电子货币的发行同传统的货币发行大体上是相同的，都应当是由国家相关机构授权某些实体发行和推广使用。然而，电子货币却又不同于传统货币，它的完全数据化以及对高科技技术的依托性，又迥异于传统货币。这就要求我们在对待电子货币发行的问题上要灵活地认识和对待。

1) 电子货币发行主体资格认定

对于主体资格的认定是很有必要的，因为它是电子货币授权发行的前提和基础。一般认为，电子货币的发行主体在其经营条件上要与传统的信用金融机构相同。因为就目前发展而言，在电子货币的发行条件上要依靠传统货币发行的模式要求不能脱离，当然就发行环境而言也是不应该脱离。在主体的经营分类上必须规定其可以从事的商业活动类别，以方便管理监督，防止金融欺诈。在其主体申报审查中，要采用预先审批的办法，其注册资本、投资限额、发行量等都应明确作出规定。特别是在资本运作上，要有足够的在线资金做好风险防范，以防止在突发事件面前侵害到消费者的合法权益。如随时满足用户的资金划拨与兑现。更不能虚夸运作资本，要在资金、信誉上有充分的保证、保险。电子货币的发行实体必须接受国家的统一监督与管理，做好定期的审查和汇报。此外，发行主体还必须提供出保证整体经营系统安全的保障。

2) 电子货币发行主体的范围规划

如何确定电子货币的发行主体、如何规划发行主体的范围，即在宏观上确定电子货币发行的授权对象，这无论是对电子货币的发行、监管，还是促进其良性发展，都是一个根本性的问题。由于电子货币还处于起步时期，还有很多设施及技术不太成熟、完善。因此，传统的金融机构、传统的金融信用机构经审查合格者一般都可以进行电子货币的发行。这些信用机构可以是专门做电子货币发行的金融实体，也可以是既做传统性现金货币，又做电子货币的金融实体，只要在主体资格认定上符合相关要求。此外，为了电子货币的长足发展，还可以适当的鼓励民间资本及信用机构参股到电子货币的发行中来，为今后电子货币的广范围、宽领域发展打下基础。当然，在针对特殊实体的加入，如民间金融、私营资本等，要有相关政策的制定，既不能过于苛刻，又不能低于实体资格认定标准。太严谨会打消那些特殊信用实体发展电子货币的积极性，不利于其发展；过于疏松，就会给电子货币的发行带来无序性，会出现鱼目混珠的现象。

2. 电子货币发行实际要求

电子货币还是不成熟的货币，正处于起步阶段，但在未来的经济发展中有着举足轻重的作用。为了其以后的良性发展，应在电子货币发行的实际运作、整体发行要求与方式上有统一的认识。电子货币的发行中应在客观上把握以下两点。

1) 统一发行规范与尺度

电子货币的发行过程中要设立或执行一个统一的标准，这个标准需要由国家的相关职能部门或机构来制定。它不仅是在电子货币的发行整体范畴上制定出一个标准，而且还应该针对每一个发行环节上制定，即它应包括所有的电子货币发行所涉及的，如发行类别、

发行金额、软件系统平台和安全要求等。任何的金融信用实体在发行中，在技术、管理以及程序上都要按照标准统一部署，便于监管防止在电子货币交易中可能出现的交易无序性、重复性等问题。

2) 实行发行集中制

就目前电子货币的状态来分析，无论是从其表现形式及发展势态上看，还是从技术的应用角度分析，电子货币仍处于发展中的新生状态。因此，特别是在其发行方式和程序上应进行较为谨慎的探讨，结合现实操作制定出合理的、规范的发行机制和监管机制，以保护消费者权益免受侵害。因此，在电子货币的推广发行中，认为应该实行像传统货币发行的集中制模式，由国家相关职能机构监督，由中央银行向其他商业银行、金融信用机构进行授权发行。类似于法币的发行，但又不同于法币的发行体制。法币是直接由国家中央银行被授权发行，在资金结算上中央银行与各商业银行和金融机构之间实行二级模式，即中央银行与商业银行间、商业银行与社会各金融信用机构间进行分离的结算划拨。而在这方面，电子货币只需采用一级模式，即直接授权操作，由中央银行授权于商业银行和金融实体，实行直接接触的一次划拨。这样，即方便相关机构监管，也可以确保结算系统安全可靠、发行一体的财务运作及管理的完善健全。还可以尽量减少电子货币在发行以及流通中出现的漏洞和失误。因此，可以通过适当的立法规范，把电子货币作为未来的第二“法币”，确立起其法律地位。

3. 发行的管理

由于电子货币在相当程度上有着类似于现金的特征，其发行将无疑减少中央银行货币的发行量，影响中央银行发行货币的特权。对于无国界的电子商务应用而言，电子货币还在税收、外汇汇率、货币供应和金融风险等方面存在大量潜在的问题。因此，必须制定严格的电子货币的发行管理制度，保证电子货币的正常运作。

为保证电子货币的发行机构保持必要的流动性和安全性，中央银行可以采取以下措施实施管理。

(1) 向所有的电子货币发行机构提出储备要求和充足资本要求。

(2) 应当建立电子货币系统统计和信息披露制度、现场和非现场检查制度及信息安全审核制度。

(3) 建立安全保障体系。目前，许多国家正考虑建立电子货币的担保、保险或者其他损失分担机制。其中，美国、德国、日本、加拿大和意大利等国家将电子货币纳入存款保险或者担保制度的体系中。

4. 关于电子货币发行监管的法律规定

目前，许多国家正在探索一种合适的电子货币发行的监管办法。1998 年欧盟委员会就规定，发行电子货币的机构与传统意义上的信用机构享有同样的市场准入权利和同等的竞争条件，电子货币发行机构只接受设立地成员国一国的管理和监督。美国和英国则认为若对电子货币的发行主体进行严格的监管和限制，会损害民间机构的技术开发和创造精神，把电子货币的发行限定于金融机构还为时过早，一些证券公司、特殊贷款公司、非银行支付供应商、信用机构也能提供电子货币服务。我国关于电子货币发行监管方面的法律主要

是《银行卡业务管理办法》，该法规定只有商业银行(含邮政金融机构)是合法的银行卡发行主体。至于对所有电子货币尤其是数字现金的发行尚无相应的法律法规。

8.1.4 关于电子货币的立法建议

面对电子货币的发展所带来的法律上的挑战，我们应当运用法律积极加以解决。

1. 通过立法适当限制电子货币的发行主体

电子货币的发展，应靠市场的力量，而不是在当前就用强制的方式指定由谁来发行或经营从而阻碍电子货币的发展。只要能提供安全可靠的技术系统和强大的商业信用，所提供的电子货币符合货币的使用特征，就应允许其发行电子货币。通过限制发行主体的准入条件，从源头上控制电子货币的风险。

2. 以法律的形式确定电子货币相关方的权利和义务

根据电子货币的发展，研究、制定和明确电子货币规范化运作的一系列相关法律法规，明确界定电子货币涉及的各方当事人的权利、义务范围以及争端解决机制，以解决目前电子货币交易过程中各方权责不清的现象，保护各方的正当权益，一旦发生纠纷时能够追究相应的责任。

3. 加强对电子货币隐私权的保障

对于隐私权保护方面要明确规定以下内容：电子货币发行主体不能采取非法方式收集个人资料；对于合法收集的资料不能用于所声明的目的以外的事项；电子货币使用人有知情权，有权知晓资料收集人的身份、收集的目的、使用的方式和资料的保管；电子货币使用人对其资料有修改、更新权；以及电子货币使用人在资料安全被侵害时的有赔偿请求权等。

4. 加强电子货币的安全控制

首先是统一电子货币的安全技术标准和认证方式，建立合理有效的电子货币识别制度。其次是电子货币的开发者、发行主体应建立内部风险控制和管理秩序，能够识别、衡量、监管和控制各种潜在的风险，防范违反安全规定的各种形式的侵入，确保信息的完整性和对消费者隐私权的保护，提供安全、可靠、可用的电子货币产品。最后是加大对网络犯罪的打击力度，保护电子货币交易各方的合法利益。

5. 完善电子货币反洗钱方面的立法

一是建立严格的身份认证制度和交易记录制度。电子货币的匿名性为洗钱犯罪带来很大便利，建议电子货币发行主体执行严格的身份认证制度，要求客户提供真实的身份认证信息。二是扩大反洗钱责任人的覆盖面。除了银行类金融机构外，承担反洗钱义务的责任人还应该包括非银行的电子货币发行主体和互联网服务提供商，督促其履行反洗钱义务，打击运用电子货币的洗钱活动。三是相关技术方面的防范措施。由于电子货币交易的纪录和追踪与电子货币的匿名性和保护公民隐私权产生矛盾，因此，可以采用不完全匿名或有条件匿名的电子现金系统。一方面，应该建立中央数据库进行追踪，记录相关交易情况。另一方面，应该通过立法的方式对个人数据的隐私权保护问题等做出明确规定，如规定哪

些机构在怎样的情况下可以取得这些数据和资料等。四是国际间的合作洗钱犯罪的跨国性特点，决定了国际间必须加强合作，才能有效地惩治和防范洗钱犯罪。国际经验表明，面对日益严重的跨国洗钱现象，任何一个国家仅靠自身的力量很难有效的预防和控制洗钱行为，必须加强反洗钱的国际合作。目前亟待开展的国际合作主要有以下几个方面：信息交流、技术共享、司法协作以及推进一项全面打击电子货币洗钱的国际公约。

8.1.5 发达国家电子货币监管实践

1. 电子货币给金融监管带来的新问题

1) 安全问题

主要指的是在使用电子货币进行支付过程中，金额、卡信息(如密码和持卡人身份认证)等信息传递的安全问题。此外，还有因商家和消费者的信用问题而带来的信用风险等。尤其是在使用以互联网或软件为基础的电子货币进行交易时，所带来的安全问题更为突出。

2) 对货币政策的影响

电子货币的发行和流通降低了货币供给中的交易成本，模糊了传统货币层次的划分，使得货币乘数变得更加难以测量。因此，中央银行使用传统的以货币供应量为中介目标的货币政策机制将受到前所未有的冲击，并最终使货币政策的有效性受到影响。

3) 法律问题

主要包括 3 个方面：一是关于电子货币发行主体的确认及发行规模、种类等的确定；二是关于电子货币交易的合法性问题；三是关于流通过程中引起的纠纷的责任识别和解决办法裁定等问题。

4) 其他问题

电子货币的广泛使用还会带来其跨国流动问题，防洗钱问题以及消费者权益的保护问题等。

2. 发达国家电子货币的监管实践

发达国家对电子货币的监管，有两种不同的态度，各自对应着不同的监管机制。

第一种以欧盟国家为代表，主张在电子货币的发展初期就建立复杂的监管体制。优点是可以降低电子货币系统的潜在风险，缺点是可能妨碍电子货币发展过程中的创新。欧盟对电子货币监管的主要目的是防止货币政策实施的滞后、维护金融市场的统一和稳定、促进支付系统高效运作。欧盟主要采取以下两种模式：一是单独建立电子货币监管部门，负责研究电子货币对金融监督、法律、消费者保护、管理、安全等问题的影响，跟踪电子货币系统发展的最新动态，提出有关电子货币发展的宏观政策建议和报告。二是现有的监督机构根据电子货币的发展状况，修改不适用于数字和网络经济时代的原有规则，同时制定一些新的监管规则和标准。

第二种以美国为代表，主张在确实有必要监管时才制定具体监管措施。这种做法为电子货币业务的参与者提供了一个宽松的环境，但这可能造成监管时机的滞后或延误，导致更大的损失。美国认为，要使监管持续有效，就必须确保私人部门存在有效的风险管理体系，随着金融系统变得越来越复杂，详细的规则和标准也将变得累赘和无效。美国在电子货币监管的法律制度建设上比较完善，美联储作为实施消费信贷法律的监管机构，曾颁布

了多部法规，这些法案基本上都是以消费者信贷保护为中心，对债权机构提出了相当苛刻而且细致的义务性条款。美国利用一系列完善的信用法律制度为信用交易提供法律保障。

总的来看，各国或地区对电子货币的监管主要集中在以下几个方面。

第一，对电子货币发行者身份的限制。在 20 世纪 90 年代中期，由于管理制度的变化落后与电子货币市场的发展，电子货币的发行者一度呈现出多元化和自发成长的特点。20 世纪 90 年代末期一些国家开始对电子货币发行者进行限制，一些学者也极力主张只有信用机构才能发行电子货币，部分国家(芬兰)甚至通过中央银行将电子货币的发行垄断起来。但随着电子货币的推广受到技术创新、投资成本、宣传费用等因素的影响，越来越多的人认识到推广电子货币必须依靠市场的力量来进行。在这种背景下，进入 21 世纪以来，对电子货币发行者的控制又出现了逐步放松的趋势。

第二，对发行电子货币预收款项的管理。发行者通过发行电子货币预收的款项，不同于一般的存款，也不同于预售产品和服务收取的预收款，它对应的是发行者的一般性责任。对这部分款项如何管理主要有以下几个问题：一是是否允许电子货币被“借贷”、多次转让和流通，如果允许的话，电子货币就有可能成为另一类的“基础货币”；二是对发行者是否应该要求交纳一定比例的准备金，以及如何测算和确定其流动性和缴纳比例；三是如何监控这些预收款的总体数量、安全性，并提供适当的风险保障措施。对于上述问题，目前还没有成熟的经验和办法，各国仍在尝试之中。

第三，电子货币系统设计与支付清算体系安全控制。电子货币系统设计不适当，不仅会对电子货币发行者带来风险，也会影响到整个支付体系的安全。许多国家和地区对电子货币系统的设计提出了较明确的要求，一般也需报中央银行审查。如，法国银行规定：在法国境内推行的电子货币，必须将发展计划呈报该行；香港金管局要求电子货币的发行者必须对电子货币发行后三年的预计发行数量、储值卡的平均储值金额、预计收到的款项、储值卡的建议使用范围、预计每年的交易价值等情况进行评估和上报，对于非金融机构发行的储值卡，必须就主要和附属用途分别评估。

第四，反“洗钱”问题。为防止电子货币被用来进行非法交易、非法转移资金和洗钱等犯罪活动，同时控制电子货币的风险，对电子货币的储值价值需要加以限定。日本主要通过法律法规对单位储值卡的最高储值进行限定，美国主要依靠发行者自行对最高储值价值进行限定。目前，电子货币仍然被限定为用于小额结算，以 Mondex 电子现金为例，在香港其最高储值金额限定在 3000 元港币。

8.1.6 加强电子货币监管的具体措施

1. 中央银行和银行监管委员会共同实施监管，将电子货币纳入金融监管体系

目前欧盟国家普遍是在中央银行或者财政部货币总署成立电子货币监管部门，跟踪电子货币系统发展的最新动态，制定监管规则和标准。而在美国，电子货币由联邦储备委员会(the Federal Reserve，FED)和货币监理署(Office of Comptroller of Currency，OCC)共同负责，由州储备银行和州政府实行分级管理。从我国当前的金融监管体制和微观金融主体来看，我国的电子货币的监管权应归属于金融监管当局，由中央银行和银行监管委员会共同实施监管，并将之纳入现行的金融监管体系，这种监管模式具有现实性和可行性，同时可

在立法上对两者的监管权限、监管职责予以协调和明确。

2. 加强对电子货币系统的审慎监管

一是对发行主体的资格认定，应严格限制为信贷机构。二是对所有电子货币发行人建立资本充足率和准备金缴纳制度，维护电子货币系统运行的流动性和稳健性。三是建立电子货币产品担保、保险或其他损失分担机制，完善电子货币发行人的退出和清算程序，以保护消费者和商户的利益，降低因电子货币失效对金融体系的冲击。四是尽快制定国内电子货币流通规则和监管制度，加强对电子货币经营与交易活动的流动性管理、清偿性管理、风险管理、安全支付标准管理和交易清算管理。

3. 构建适应信息化时代要求的电子化监管网络

要实现金融监管方式的电子化，就要建立高效、安全、功能完善的金融监管信息系统，运用人工智能技术、金融工程技术和现代统计学方法，对信息进行科学的处理与分析。电子货币监测信息系统包括电子货币数据库系统和电子货币风险监测信息系统，它对所有境内和境外发行的现金替代型和独立支付型的电子货币，建立其数据采集的强制性信息披露制度，通过风险预警体系跟踪全球信息技术的最新发展，在技术上实现电子货币风险的识别、衡量与控制，提高电子货币系统的安全性、可靠性和可用性。

4. 建立电子货币的消费者权益保护机制

监管当局必须要加快个人信用法律制度建设，建立消费者权益保护机制，切实维护消费者的正当权益，从而为电子货币的发展提供强大的法律保障。此外，也要积极推进国内统一的、公开的、有效的企业与个人信用信息系统和信用评级体系，积极发展信用中介服务机构和企业与个人信用评估机构。信用中介机构可专门从事信用资料的收集、记录、整理、分类管理，建立信用信息数据库，向成员金融机构提供所需要的个人信用状况报告。企业与个人信用评估机构由专门的金融机构或评估机构在上述信用报告的基础上，对借款人进行风险评估，建立评估体系，并提供资信评估与信贷决策服务。

5. 完善电子货币相关的法律体系

随着电子货币日新月异的发展，迫切需要配套的法律法规对电子货币系统行监管。目前，很多发达国家和国际组织已开始考虑电子货币立法的问题。我国应该根据电子货币发展的不同阶段制定相关的法律，完善电子货币规范化运作的金融法律、法规体系，建立电子货币的发行备案、信息披露制度，明确界定电子货币发行人、清算人、网络经营者和消费者等参与主体之间的责任义务、权利范围和完善纠纷处理方案。

6. 加强国际间电子货币监管的协调合作

作为网络时代的产物，电子货币使任何一笔跨越国界的巨额交易能在瞬间完成，因此电子货币监管的国际协调与合作显得更为重要。要逐步建立与现行的国际金融组织体系相适应的新规则和合乎国际标准的市场基础设施，如信息真实披露、资金实时清算和风险动态监督等，以提高金融监管的透明度和反应能力。要强化不同国家金融监管组织之间的跨国合作，严厉打击国际间的资本外逃、欺诈、逃税、洗钱等金融犯罪活动。

此外，在监管方式的选择上，应该更多的采纳监管创新模式，使电子货币更好的发挥

积极的经济促进作用。监管创新论相对于传统理论的主要区别体现在以下几个方面。

(1) 在监管方式上来看，从机构监管过渡到功能监管。由于金融经营模式由分业向混业发展，金融机构也就向着全能化发展，传统的以机构为监管对象的方式便不能再适应金融领域的发展，而应以功能为基础进行监管。

(2) 在监管标准上来看，从资本监管到全面性的风险监管。传统金融监管以银行金融机构的资本充足率为标准，这种监管主要是针对信贷风险的。但是金融创新使金融机构面临着其他各种风险，仅仅针对信贷风险进行监管难以实现有效监管的目的，而必须转向对信用风险、流动性风险等各种风险实现全面风险管理。这已经成为各国及国际监管制度发展的一个重要趋势。

(3) 内部控制制度的加强。传统金融监管制度注重外部控制制度，随着金融创新的发展，各国及国际监管机构正在对金融机构内部控制制度的健全性、有效性给予越来越高程度的重视。

电子货币作为一种金融业务，无论是由金融机构还是企业集团发行，都应当说有一定程度的货币流通性，更因为大多数电子货币都代表商业信用，发行者的运营状况对电子货币的安全与效率产生着决定性的影响，从而关系到电子货币使用人乃至整个国家金融体系的稳定运行。因此，应当对其采取一定程度的监管，对电子货币发行者进行引导和规范，对电子货币流通中出现的问题进行适当防范，协调电子货币市场各方主体的利益，在提倡发展电子货币的同时，保护消费者的合法权益，以实现国家、商户和消费者共赢的局面。

8.2 电子支付的法规和监管

阅读案例 8-2

诈骗案暴露安全漏洞

2002 年 9 月 12 日，总部位于洛杉矶的 Spitfire 投资公司在 90 分钟内收到了提交的 14 万笔信用卡业务。其中有 62477 笔被确认有效，每笔金额 5.07 美元。该公司是在接到信用卡持卡人的电话后才发现这起诈骗案的。该公司首席执行官 Paul Hynek 说：“6 万多人的信用卡账号受到入侵，而且许多人至今还蒙在鼓里。”

在线信用卡交易商 OnlineData 公司确认的虚假交易为 104000 笔，涉案交易的金额从几美分到几美元不等。Spitfire 公司网站每天通常处理 5～30 笔交易，而 9 月 12 日异常的爆发当时并未立即引起安全方面的关注。犯罪分子成功地窃取了这么多认证密码暴露出在线信用卡处理系统的安全漏洞。

资料来源：http://tech.sina.com.cn/i/2009-03-14/07022909686.shtml.

问题：

1. 鉴于上例，你认为应如何保障网络支付的安全，其中信用卡公司和监管机构分别该做哪些努力?
2. 上例给予了我们什么启示，政府应该如何努力来完善电子支付相关法规与监管制度?

电子支付建立在开放的网络环境上，这就决定了它天生具备某些不同于传统支付的硬伤，主要来自于技术方面以及其支付环境的特殊性，因此，政府有必要对电子支付做出更细致而深入的研究，从而制定出相关法律法规，本小节将重点介绍电子支付的法规与监管。

8.2.1 国内外有关电子支付的立法

1. 国外电子支付立法

(1) 美国 1978 年颁发的《电子资金划拨法》，适用于联储电划系统与消费者电子资金划拨，成为世界上最早出台的有关电子支付的专项立法。

(2) 英格兰银行在英国国内是采用《票据交换所自动收付系统清算规则》(CHAPS 清算规则)办理票据交换所自动收付系统(CHAPS)会员银行间的电子资金划拨。

(3) 欧洲中央银行在 1998 年的报告中讨论了建立电子货币系统的基本要求：严格管理，可靠明确的法律保障，技术安全保障，有效地防范洗钱等金融犯罪活动，货币统计报告，可回购，储备要求等。

在国际上关于电子支付的立法模式有两种：一种是以大陆法系国家，如法国、德国、日本等为代表的“一般法律调整”，即不就电子支付专门或间接立法，而是适用一般的法律，或以合同或惯例对之进行调整；另一种是以美国为代表的“专门立法调整”或直接立法，如美国的《统一商法典》(UCC) 4A 篇就是专门的电子支付法。

2. 我国电子支付立法

1999 年 1 月 26 日，中国人民银行颁布了《银行卡业务管理办法》，对银行信用卡、借记卡等做出规范。

2005 年 6 月 9 日，为规范和引导电子支付业务的健康发展，保障电子支付业务中当事人的合法权益，防范电子支付业务风险，确保银行和客户资金的安全，根据《中华人民共和国电子签名法》、《支付结算办法》等法规制度，中国人民银行公布《电子支付指引(征求意见稿)》。

电子支付立法首先要解决的问题是电子支付或无纸化支付带来的新问题。这不仅要确立电子支付的法律效力，确立形式要件、当事人之间的关系，对电子支付当事人的权利、义务和责任，电子货币的法律地位、争议解决办法、风险分担制度作出了明确的规定，而且要保障这种新的支付形式的安全性，解决数字签名和认证、传输或系统错误、信用风险等问题。

通过在各种相关法律问题的解决过程中不断改进和完善，归纳和总结，逐步实现我国电子支付的完整法律体系。

8.2.2 电子支付指引(第一号)

2005 年 10 月 26 日，中国人民银行发布了《电子支付指引(第一号)》(简称《指引》)，对银行从事电子支付业务提出指导性要求，以规范和引导电子支付的发展。

1. 制定《指引》的目的和意义

近年来，我国的电子支付发展非常迅速，新兴电子支付工具不断出现，电子支付交易量

不断提高，逐步成为我国零售支付体系的重要组成部分。因此，迫切要求对电子支付活动的业务规则、操作规范、交易认证方式、风险控制、参与各方的权利义务等问题进行规范，从而防范支付风险，维护电子支付交易参与者的合法权益，确保银行和客户资金的安全。

目前，我国电子支付业务处于创新发展时期，而涉及电子支付业务的许多法律制度问题仍然处于研究和探索阶段。为了给电子支付业务的创新和发展创造较为宽松的制度环境，促进电子支付效率的提高，保障电子支付安全，本着在发展中规范，以规范促进发展的指导思想，人民银行决定先通过《指引》这种规范性文件的方式，引导和规范电子支付行为，待条件成熟后再上升至相应的部门规章或法律法规。

《指引》的实施将有利于规范电子支付活动，推动电子银行业务和电子商务的健康、有序发展；有利于明确电子支付活动参与各方的权利义务，防范支付风险；有利于推动支付工具创新，提升支付服务质量；有利于防范和打击洗钱及其他金融违法犯罪活动。

2. 关于客户个人资料的保护问题

在几乎什么都可以信息化的时代，有关个人的信息似乎是一个非常广义的概念，比如一个鲜为人知的私生活也可以是一种信息，将之公布于众，也是对个人隐私权的侵犯。在网络环境下，个人资料不仅仅指不适宜或不愿意公开的信息，而且包括了不属于民法隐私范畴的信息，如个人身份证号、国籍等信息。可以说它是以是否能够识别某个主体为标准的，而不再是以不宜公开为标准。个人资料作为隐私权的组织部分，个人享有排他支配权力，任何他人都不能侵犯或使用，否则将承担侵权责任。但是如果资料收集者基于法定的理由或当事人事先同意而收集、使用，那么在资料收集利用与资料提供者之间会产生一些因使用个人资料而产生的法律关系。

在电子支付中，银行与客户的关系构成了资料收集者与资料提供者的合同或契约关系。《电子支付指引(第一号)》明确规定了银行作为资料收集者应该承担的义务。

第九条：银行应按会计档案的管理要求妥善保存客户的申请资料，保存期限至该客户撤销电子支付业务后 5 年。

第十一条：银行要求客户提供有关资料信息时，应告知客户所提供信息的使用目的和范围、安全保护措施以及客户未提供或未真实提供相关资料信息的后果。

第二十六条：银行应确保电子支付业务处理系统的安全性，保证重要交易数据的不可抵赖性、数据存储的完整性、客户身份的真实性，并妥善管理在电子支付业务处理系统中使用的密码、密钥等认证数据。

第二十七条：银行使用客户资料、交易记录等，不得超出法律法规许可和客户授权的范围。银行应依法对客户的资料信息、交易记录等保密。除国家法律、行政法规另有规定外，银行应当拒绝除客户本人以外的任何单位或个人的查询。

第三十条：银行应采取必要措施为电子支付交易数据保密：(一)对电子支付交易数据的访问须经合理授权和确认；(二)电子支付交易数据须以安全方式保存， 并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取；(三)第三方获取电子支付交易数据必须符合有关法律法规的规定以及银行关于数据使用和保护的标准与控制制度；(四)对电子支付交易数据的访问均须登记，并确保该登记不被篡改。

第四十一条：由于银行保管、使用不当，导致客户资料信息被泄露或篡改的，银行应

采取有效措施防止因此造成客户损失，并及时通知和协助客户补救。

由上述规定可以看出，《电子支付指引(第一号)》明确指出了银行利用客户个人资料应尽的义务主要有 3 点。第一，告知义务。银行收集客户个人资料必须告知其资料处理的目的、当事人如不提供资料的后果、当事人查询及更正资料的权利等。第二，合法处理义务。《电子支付指引(第一号)》规定银行必须确保客户个人资料在公平合法的情况下处理。第三，安全保管或保存义务。《电子支付指引(第一号)》规定银行安全保存客户个人资料，防止他人盗取、删改、销毁等。

3. 关于客户损失分担问题

盗用资金所有人的密码及相关信息进行非法划拨是网络支付面临的一大安全隐患。由此产生的损失应该由银行还是客户自身承担责任，对此，《电子支付指引(第一号)》对银行从事电子支付活动提出了指导性要求，并规定：由于银行保管、使用不当，因银行自身系统、内控制度或为其提供服务的第三方服务机构的原因，造成客户损失的，银行应按约定予以赔偿。

众所周知，由于多年来银行与客户之间的非均衡地位，两者关系在市场，或者说在银行所提供的服务关系中，客户一直处于弱者的地位。银行不仅不能为客户提供优质合格的日常服务，而且就是在由于银行过错造成客户损失的情况下，要想得到赔偿也可能会有不少困难。因而在此前提下，央行在《电子支付指引(第一号)》中对银行职责的规定，无疑说是一个银行客户的福音。

然而，需要注意的是，虽然《电子支付指引(第一号)》有明文规定银行过错的几种情况，可却同时规定了“按约定予以赔偿”的条款。这就使得该项规定有落空的危险，因为在银行与客户当前现存的不平等关系情况下，如将“约定”作为赔偿原则，那银行就很可能会出于利益上的考虑，在与客户约定赔偿条件时，本能地利用自身的强势地位，迫使或变相迫使客户接受一些“不平等”的赔偿前提条款，从而在实际赔偿时，使银行责任得到减轻、甚至免除。

在这个问题上，《统一商法典》(UCC)4A 编中相关规定值得借鉴。美国《统一商法典》规定：“如果银行与其客户达成协议，同意以作为发送人的客户的名义签发给该银行的支付命令的真实性将根据安全程序来证实”，并且该安全程序是合理的，银行也遵循了安全程序的规则，善意的接收了支付指令，那么一项经过了安全程序的未经授权的电子支付仍视为授权的和证实的支付命令，由此造成的损失由客户承担。但是，如果客户能够举证，电子支付指令不是由能够接近安全程序的客户雇员或其代理人发出的，也不是从客户可以控制的来源发出的，即使支付指令经过了安全认证程序，客户造成的损失也将由银行承担。

从美国的相关法律规定中可以看出，对于客户损失的责任承担问题，美国适用的是“公平责任原则”，将客户的损失有条件的在客户和银行之间进行分担，可以说是欲在客户和银行利益之间寻求一种平衡，从而促进电子支付服务的发展。从美国的法律反观我国，对中国人民银行来说，在设计客户损失分担的行政规范时，既要考虑具体条款行文，也要考虑该条款具体施行时可能出现的情况，并一一予以安排。如此才能体现制度的公正，也才能使相应条款在实践中具体落实。

4. 关于电子支付风险规避的问题

关于电子支付风险规避的问题，《电子支付指引(第一号)》主要通过如下规定尽可能减少风险。

第二十三条：银行开展电子支付业务采用的信息安全标准、技术标准、业务标准等应当符合有关规定。

第二十四条：银行应针对与电子支付业务活动相关的风险，建立有效的管理制度。

第二十五条：银行应根据审慎性原则并针对不同客户，在电子支付类型、单笔支付金额和每日累计支付金额等方面作出合理限制。银行通过互联网为个人客户办理电子支付业务，除采用数字证书、电子签名等安全认证方式外，单笔金额不应超过 1000 元人民币，每日累计金额不应超过 5000 元人民币。银行为客户办理电子支付业务，单位客户从其银行结算账户支付给个人银行结算账户的款项，其单笔金额不得超过 5 万元人民币，但银行与客户通过协议约定，能够事先提供有效付款依据的除外。

这种限额的做法有利也有弊，有利的一面是如《电子支付指引(第一号)》所言“规范电子支付业务，防范支付风险，保证资金安全，维护银行及其客户在电子支付活动中的合法权益，促进电子支付业务健康发展”，明显地看出对银行是很有利的，提高电子支付的安全性，降低电子支付业务的风险。不利的一面也很明确，那就是增加了客户网上购物、电子商务的难度及复杂度，对银行客户是不利的。此外， 限制策略对防范风险所起的作用也非常有限。

《电子支付指引(第一号)》中的限制策略只起到一旦被骗客户损失数额相比以前有大大减少的可能性，对提高电子支付的安全性作用不明显。因此， 对于电子支付风险规避问题，应该从加强客户防范意识和银行内部控制以及改善外部环境等方面着手解决，而不是仅仅从交易额方面严加限制。这也是今后电子商务立法应该考虑的问题。

8.2.3 网络支付的法律关系问题

1. 网络支付主要参与人

网络支付活动中涉及的当事人主要有以下几类：客户，其中又包括消费者(个人消费者或企业集团)和网上商户(包括制造者、销售者和其他服务业者)、第三方支付服务商(第三方支付平台)、网上银行。

1) 消费者

消费者是指通过 Internet 购买了商品或服务引发了需要向商家支付款项的债务，消费者用自己拥有的支付工具(如信用卡、电子钱包等)来发起支付，是支付体系运作的原因和起点。通常将电子商务中的客户在网络支付环节的角色定义为付款人，是整个网络支付活动中第一个发出资金支付指令的人。

2) 网上商户

网上商户是拥有债权的商品交易的另一方，通常是电子商务活动中产品、服务的提供方。他可以根据消费者发起的支付命令向金融体系或第三方支付服务商请求获取货币给付。其角色是收款人，在整个网络支付活动中支付资金的受益人，资金按指令被划拨至收款人处则一个完整的网络支付过程结束。

3) 第三方支付服务商

由于网上银行和网上商户、消费者之间关于支付请求有着不同的协议，目前没有一套兼容的标准，在一定范围内形成垄断，对网络支付的发展起到阻碍作用。于是出现很多以第三方角色出现的支付服务提供商，主要有第三方支付平台以及银行支付网关。第三方支付平台，其主要功能是连接买卖双方、电子商务平台和银行，起到一个桥梁作用，最终实现网上交易的资金划拨。商业银行通过第三支付平台建立支付网关，相关的网络支付指令通过银行网关最终进入银行的后台处理系统，进行资金的最终处理。

4) 网上银行

网上银行是电子商务的参与者，它与买卖双方一样通过电子手段连接在网络中。但是银行与电子商务的买卖双方地位并不相同，买卖双方在电子商务中拥有贸易自主权，而银行只是买卖双方完成商务活动的服务机构，其服务主要体现在货币资金支付与清算等功能上。此外，第三方支付模式下的参与人还包括网上交易平台服务提供者、认证机构等。

2. 网络支付当事人之间权利义务关系及相关法律问题分析

1) 消费者与商户的关系

网络支付中的基础法律关系是买卖双方之间，即消费者与商户之间的关系。消费者与商户通过网络支付形成相应的债权债务关系，存在着合同关系。双方的买卖合同在支付环节双方身份即表现为付款人和收款人。这是传统意义上的债权债务关系，付款人有义务在合同规定的时间内向收款人支付货款，并有权获得相应的货物；而收款人则有权在合同规定的时间内取得该笔货款，并负有交付货物的义务。网上购物的整个合同关系，从要约、承诺到合同的订立直至合同的完全履行，整个过程有时仅需短短几分钟就可以完成。但网络支付的顺利进行必须以买卖双方之间的基础法律关系为基础，才能进行有效的资金划拨。

2) 客户与网上银行的关系

在网络支付过程中，银行与客户之间的权利义务关系是通过银行卡使用协议和网上银行协议来确定的。他们之间的关系也可归结为合同关系。这里的合同关系有其独特之处(引自《网上银行法律关系研究》，王国存)：其一，合同的形成是无纸化的过程， 即当事人之间通常不需要纸化的要约与承诺形式; 其二， 当事人之间交易契约形成往往以一定的“预先交流”为前提， 因为银行通常要求客户履行一定的申请手续或要求客户预先授权; 其三， 要约与承诺生效的瞬时性， 即客户向银行发出的指令及银行接受指令并按指令行事都可能在瞬间完成， 客户很难撤回自己的指令; 其四， 银行与客户之间的权利义务关系具有较强的恒定性和明确性， 因为客户在与银行确立关系时， 双方之间的基本权利义务就已经大致明确，具体交易中的权利与义务有许多类似之处; 其五，在交易关系中，银行始终处于主导地位， 这主要表现在银行掌握交易规则的制定权、控制了交易设施及交易的有关信息等。

根据合同，消费者即付款方有权要求银行按照其指令将指定的金额支付给商户即收款方，对于银行未按指令执行或其他违约导致的损失有请求赔偿的权利。收款方则有权要求银行对付款方支付并划拨的资金进行妥善保管，并对银行的违约导致的损失有请求赔偿的权利。银行有权向用户收取执行支付指令期间的手续费，并可以对付款方不符合规定程序的支付指令拒绝执行或要求其修改。其相应的义务可由上述权利推论得出，这里不再赘述。

在银行和买卖双方之间，其合同形式以格式合同为主，而格式合同均由银行起草提供，通常银行对其赔偿责任规定数额限制，而用户因处于弱势地位，难以更改协议中银行的免除或限制责任条款，权利难以得到充分保障。对于这一问题，将在后文进行分析。

3) 消费者与第三方支付服务商的关系

从表面上看，第三方支付服务商不参与交易，仅仅是为消费者和商家提供了一个支付平台。但是，当前第三方支付平台基本上与消费者都有服务协议。如消费者在淘宝网上若想使用其在线支付工具——“支付宝”，则必须与其签订“支付宝服务协议”，因此第三方支付服务商与消费者是一种网络服务合同关系，双方的权利、义务关系受该服务协议调整和约束。但需要指出的是，这类协议基本上都是第三方支付服务商提供的格式合同，消费者对该协议条款“要么全盘接受，要么就走开”，没有协商余地。因此如何对该类格式合同进行规制，加强对消费者的保护，也是立法所需要注意的。

第三方支付平台与消费者之间的服务内容主要集中于确保商家主体资格真实性、消费者个人信息和支付安全 3 个方面。

确保平台商家的真实性义务：第三方支付平台对商家主体资格有进行形式审查义务。作为中介，消费者是基于对第三方支付平台的信任而采用第三方支付，因此第三方支付平台应对其平台上的商家的身份进行核实，当然，这种身份核实仅仅是形式上的，也就是说只审查商家依国家法律取得主体资格，是合法注册的真实企业，主要审查营业执照、许可证等法律资格，但对其经营状况、资信状况、出售产品的质量等不承担任何认证或保证义务。

消费者欲使用第三方支付，一般都需要注册为第三方支付平台的用户，而这些注册信息涉及消费者的个人隐私，第三方支付平台应当为其保密，如果这些信息用作其他用途，消费者有知情权，哪些信息被使用以及用作什么用途，消费者有确认和选择权。第三方支付平台应当采取必要措施加以保护，不得侵犯消费者的隐私权。

消费者网上交易最担心的就是支付安全问题，担心自己的信用卡信息被滥用，或者货款被不当支付。在第三方支付模式中，第三方支付平台充当一个桥梁的作用，消费者通过该平台在相关银行网关输入支付信息，因此，第三方支付平台应当采取措施保证信息的安全。此外，第三方支付平台应当严格按照消费者的支付指令划拨资金，不能未经授权错误划拨，如果因第三方支付平台的过错，导致消费者权益受损，应当承担赔偿责任。

4) 第三方支付服务商与网上商户的关系

第三方支付平台与网上商家也是通过“支付服务协议”建立服务关系的，因此双方权利、义务也受该协议的调整。

对第三方支付平台而言(如“首信易支付”、“支付宝”等)，其商家类型基本上有两种：一种是直接从事 B2C 交易的商家，一种是交易平台型的商家。这两类商家的不同在于，交易平台型的商家是为他人销售或从事在线经营提供交易平台服务的，它本身不从事在线销售或服务；这样，平台型商家成为第三方支付平台的客户也间接地使其平台上的商家成为第三方支付平台的客户。因此商家应当在其网站上明示其网站上的在线交易的支付服务是由第三方支付平台提供的，有关支付服务应当遵守第三方支付服务协议。

对于第三方支付平台而言，区分这两种平台的意义在于，第三方支付平台对消费者所负的保证其平台上的商家真实性义务，不能延伸到交易平台上的商家。至于该交易平台上

的商家的合法性、真实性的保证义务是由平台经营者自己承担。

此外，上文所述的消费者与第三方支付平台关系中所涉及的格式合同、资金错误划拨等问题，在第三方支付平台与网上商户的法律关系也存在。

5) 第三方支付服务商与网上银行的关系

在第三方支付模式中，第三方支付平台实际上成为商家的直接付款人，消费者的货款是先经过第三方支付平台的银行账户，再由第三方支付平台的账户转账到商家的银行账户。上述两个阶段的实现以及整个支付流程的运行都需要金融机构的合作。第三方支付平台与银行之间通过金融服务协议建立服务合作关系。

如以支付宝为例，在第一阶段中，消费者在线支付，同时支付宝基于协议有权要求该银行卡(目前国内各银行仅允许凭借记卡申请开通网上银行的虚拟“电子支付卡”)的发行银行确认银行卡的真伪及金额。银行确认后，便按支付宝的指令将相应货款划拨到支付宝的银行账户上。在此阶段，银行的主要义务是：①对消费者银行卡的认证；②按支付宝的指令(实际上原始指令人为消费者)完成资金的划拨。银行的主要权利是：拒绝或要求指令人修正其发出的无法执行的、不符合规定程序和要求的指令。

在第二阶段中，消费者的货款由银行转至支付宝的银行账户中，待支付宝明确消费者已收到货物并同意支付货款，便通知银行将存放在其账户的货款(扣除服务费)划拨到商家的银行账户上。在此阶段，银行的主要义务就是按支付宝的指令划拨资金。

综上所述，在网络支付活动中，支付服务提供商并非必要当事方；但由于网上银行的数量较多且存在着互不通用的障碍，在现阶段电子商务发展中，致力于网络支付服务的中介机构(如第三方支付服务商)对网络支付的推广应用起到了极大的促进作用。中介机构和网上银行的关系应该是代理关系，中介机构是代理人，通过代理网上银行与其服务使用对象(网上商户、消费者)发生关系，此关系应受民法代理制度调整。同时，他们之间的合同也应适用《合同法》的调整。网上银行与支付服务提供商之间比较容易引发对系统故障、电子信息错误，未授权的支付命令的责任承担等法律问题。

3. 网络支付法律关系调整的基本原则

1) 应当确立充分利用已有法律体系、视情逐步完善的立法原则

虽然网络支付的发展带来许多新的法律问题，给现有法律体系造成较大冲击，但笔者认为网络支付本身仍然是支付活动，仍然应当受到现行法律的调整。网络支付较之传统支付方式的改变主要在于它的网络化，对于这种改变应当尽量通过对传统法律规则进行调整或修改的方式，使其融入现行的法律体制中，而非重新确立一套新体系、新规则。对于现行法律确实无法调整、修改的问题，可以寻求制定新法律的方式来解决。

2) 应当确立自治规范和立法规范双轨制原则

目前，我国网络支付业务处于创新发展时期，第三方支付的异军突起，也显示了其对突破网络支付“瓶颈”、促进电子商务发展的重要作用，因此对于网络支付这个新兴行业，笔者认为政府应当加强宏观指导，营造发展环境，促进产业发展。由于网络支付具有发展迅速、涉及范围广、形式多样、技术性强等特点，政府应当避免对网络支付作不恰当的限制，可以容许商业性探索，鼓励行业进行一定程度的自治，让业界共同参与政策法规的探讨和制定。从而实现在发展中规范，以规范促进发展的目标。

8.2.4 电子支付的监管

(1) 欧盟的电子支付监管：主要针对电子货币进行立法，1998 年、2000 年、2002 年欧盟颁布了指导欧盟各国的电子货币与电子支付一系列法律文本。强调对消费者的保护，严格准入条件，一旦准入便可陆续在欧盟各国通行。至 2009 年为止，欧盟有 6 个国家共颁发 12 张电子货币机构执照，7 个国家 72 个实体申请以小规模方式运营，注册于英国的运营商最多。在线支付与公交支付是主要业务。至 2005 年年底，流通中电子货币总量银行占 60%，非金融机构占 40%，总的发展情况比预期的稍慢。

(2) 美国的电子支付监管：与欧盟不同的是美国则以相当宽松的态度对待电子货币与创新电子支付服务，既没有专门针对电子货币立法也没有对电子货币给出单独的定义。如储值卡、智能卡、电子钱包这类产品被看做债务而非储蓄，因而允许非银行机构发行这类支付工具。对非银行电子货币发行商的监管责任主要在各州，受到货币转账或货币服务业务法律所监管，大多有资本金、储备金、执照方面的限制。由于其宽松的态度，出现了如 PayPal 这样的第三方电子支付服务公司。

(3) 亚洲的电子支付监管：新加坡鼓励在本国发展电子支付，一方面维持原有弹性审慎监管原则，另外通过适时而不是单独立法来指导和促进其发展，包括宽松的虚拟银行设立。而印度，则不准设立虚拟银行，业务限制也很严，也限制外国机构在印度进行电子支付业务。香港地区在电子支付准入方面要求也类似印度，在业务方面则非常宽松。日本则对本国电子支付机构非常宽松，对外国电子支付机构限制非常严格。

(4) 我国的电子支付监管：尚缺相应的监管办法。《电子支付指引(第一号)》主要针对金融机构的电子支付进行了一些约束。在这个《指引》出台前，商业银行在电子支付整个业务流程、技术风险防范、业务规则、信息披露、消费者权益保护等方面都还没有一个很好的规范。采取《指引》的方式，并不是强制性的。《电子支付指引(第一号)》对非金融机构的第三方电子支付及电子商务支付没有任何约束，这些组织未能得到有效管理，既不利于风险控制，也不利于这些机构的发展。

《支付清算组织管理办法》虽然明确了非金融机构从事电子支付的门槛，但也有如下不足：对于网络支付服务商，如第三方支付网关，本质上是使用银行提供的服务，而非向银行提供跨行交换服务，划入支付清算组织未必一定合适，也就是说第三方支付机构是不是金融机构问题，如果不是金融机构，采用金融机构管理方式合不合适。网络支付服务以及各类零售与行业支付工具、移动支付以及无线支付等电子支付服务应当被监管，但策略上应找到更恰当的办法。笔者认为第三方支付服务商的监管重点更应当放在服务是否构成银行(储蓄)业务、公司信息披露的要求、审计的要求、零售业务中消费者保护的要求等。

8.3 网络银行的法规与监管

为什么网络银行需要相关的法规进行监管，又应当如何进行监管？本节就该问题重点分析。

阅读案例 8-3

黑客盗取网银信息网上廉价出售

2009 年央视 315 晚会曝光一名叫“顶狐”的黑客，通过自己制造木马程序，盗取大量用户的网上银行信息，用很低廉的价格在网上出售，危及大量网银用户的安全。

“顶狐”通过木马程序，盗取个人的网银信息，后对盗取回来的信息分类整理，将密码等信息廉价出售，而网上银行用户信息则以 400 元每 G 的价格打包售出。这导致大量的网银用户存款被盗。

“顶狐”是一名黑客高手，2006 年他编写了木马程序，从此开始了盗取个人信息的行当。该程序还以免费下载的方式任由人下载和传播，“顶狐”偷偷给自己留了一手，黑客们盗取的所有信息都会自动回复到他的手中。每天存储在他电脑上的信息有 3G，相当于 15 亿个汉字的信息量。

在国外也有类似的案例，瑞典最大银行北欧金融集团自 2006 年 9 月至今多次被一犯罪团伙利用互联网进行诈骗，诈骗金额高达 800 万瑞典克朗(1 美元约合 7.1 克朗) ，这是瑞典有史以来情节最严重且金额最大的一次针对银行的诈骗活动。斯德哥尔摩警察局宣布，已有两名重要嫌疑犯被逮捕，另有 121 人被列为嫌疑人。瑞典警方怀疑这次诈骗活动的幕后黑手是俄罗斯的有组织犯罪集团。在这一系列的诈骗活动中，共有 250 多个储户被骗。罪犯的犯罪手法狡诈，他们通过电子邮件引诱用户在他们伪造的银行主页上提供自己的银行信息。储户在提供相应资料后，便会收到该页面技术错误的提示，而罪犯则使用“特洛伊木马”病毒程序窃取储户信息。之后，罪犯迅速使用窃取来的储户信息，通过网上银行登录进入该储户的账号并转移全部资金。

银行风险作为银行的固有附随，伴随着银行的产生而存在。既然是传统银行的延伸，网络银行就必然在经营中带有传统银行的各种风险。而网络银行同时又是建立在开放网络上的银行，其风险又带有自身的特性。充分认识网络银行的法律风险及其特征，分析其根源，对加强监管、制定防范风险的措施和法规有着重要的理论和实践意义。

资料来源：http://tech.163.com/09/0315/21/54FP3QKF000915BF.html.

问题:

1. 对于上例中这种通过技术手段进行的犯罪活动而言，打击起来会遇到哪些困难？银行的责任该如何界定？

2. 你认为要针对这类风险，监管机构制定法律的要点应该有哪些？

通过阅读案例 8-3 发现，由于网络银行建立于开放网络这一环境，使其天生拥有某些传统银行所不具有的风险，这些风险主要来自于技术漏洞。因此，作为立法和监管机构，深入的调查和了解网络银行的特殊性，制定出有利于网络银行健康发展的法律法规就显得尤为重要。当然，国内外相关机构组织自网络银行诞生以来一直致力于这一领域的探讨和实践，目前为止，已经建立起了相关的法律体系。

8.3.1 网络银行相关国际法律法规现状

1. 安全套接协议 SSL

SSL 协议是由网景(Netscape)公司研制的一种对计算机之间整个会话过程进行加密的安全通信协议，采用公开密钥和私有密钥两种方法进行网络安全管理。SSL 协议能够对信用卡和客户私人信息提供较为安全的保护。

2. 安全电子交易协议 SET

1997 年 12 月，维萨卡和万事达卡公司联合开发了安全电子交易协议 SET。SET 协议的目的是为了解决用户、企业和银行之间通过信用卡支付的交易安全性，保证支付信息的机密、支付过程的完整、商户和持卡人的身份合法以及简捷的可操作性等。其核心技术包括公开密钥加密、电子数字签名、电子信封和电子安全证书等。

3. 身份认证的 CA 体系

CA(Certification Authority，认证中心)在电子商务中的显赫地位基本上是由电子商务的主流协议——SET 确定的。在 SET 中，CA 被定义为一组权威的资格认证机构。CA 通过在线或离线方式对申请加入者进行资格审查，对合乎条件的(真实可信、有信用的)申请者发放数字化的证书。CA 是与具体交易行为无关的第三方机构或组织，交易范围越广泛，所需的 CA 权威性就越高，反过来也一样。在具体措施上，网络银行的 CA 认证机制只安装在客户的个人计算机上，即使信用卡遗失了，第三方也无法用它进行网上购物，除非第三方窃取了客户的信用卡号、密码和数字证书，然而，发生这种情况的概率是极小的。

4.《电子商务示范法》

世界贸易组织委员会于 1996 年通过《电子商务示范法》，适用于在商业活动方面使用的一项资料。作为国际组织制定的统一规则，必然对各国的国内法产生重要影响。该示范法还明确规定，对本法做出解释时，应考虑到其国际渊源以及促进其统一适用和遵守诚信的必要性。

5.《全球电子商务纲要》

1997 年，克林顿总统颁布了美国政府的电子商务政策，称为《全球电子商务纲要》，其中将法律作为一个重要部分。法律部分包括的内容：在互联网网上开展商务活动的“美国统一商法典(UUC)”；知识产权的保护；个人隐私；安全；欧盟电子商务行动方案。

8.3.2 网络银行的法律风险

所谓网络银行的法律风险，是指违反、不遵从或无法遵从法律、法规、规章、惯例或伦理标准而给网络银行所造成的风险。法律风险使金融机构面临着罚款、赔偿和合同失效的风险。法律风险将导致信誉的贬低、免赔限额的降低、业务机会的受限制、拓展潜力的降低以及缺乏合同的可实施性等。其主要表现为以下几种情形。

1. 运用电子货币支付手段的法律风险

在交易规则上，针对网络银行使用电子货币的电子化结算服务，应通过法律手段加以规范。根据《中华人民共和国票据法》规定，客户委托银行办理资金转账，必须填写一定要素的书面结算凭证，并在结算凭证上签章。但网络银行办理时，客户终端屏幕上的文字和传送中的数据取代了书面凭证，密码代替了签章，其形式完全不同于现行这方面的法律要求。面对诸种差异，如不从法律角度予以认证，网络银行在办理网上货币支付时将面临法律风险。

2. 网络运行过程中产生的法律责任风险

在使用电子货币的电子化结算服务中，对有关服务承担者的资格、交易双方当事人权责以及消费者权益保护等方面，都应做出明确的法律规范，但目前尚未有明确的配套法律法规与之相适应。如在进行支付结算业务时，其实首先要支付指令通过通信系统或互联网送到银行计算机系统，经过认证系统和网关后才能完成。其中各相关的机构和服务商都对业务的实现起着关键的作用。基于此种服务和作用，它们虽与银行客户之间无契约上的法律关系，但其间无疑已形成一种事实上的法律关系。然而，它们的法律地位如何确定，应承担怎样的法律责任，在现行法律中还难以找到依据。一旦出现纠纷，将对银行的法律责任纠缠不清。

3. 银行客户隐私权及各权益被侵害的法律风险

网络银行可能因为使用电子货币和提供虚拟金融服务业务而涉及客户隐私权的保护问题，并有可能间接导致客户现实利益受到侵害，从而陷入各种商业法律的诉讼纠纷中。但目前法律对网络运行和业务操作过程中出现的消费者权益保护和隐私权保护问题都没有做出相应规定，从而使网络银行面临着相当大的法律风险。

4. 境外业务中的法律冲突风险

由于互联网本身的特性，网络银行业务和客户可随其延伸至世界的任何角落。这就向传统的基于自然疆界和纸质合约基础上的法律法规提出了挑战，主要反映在以下几个点：①跨境网上金融服务交易的管辖权、法律适用性问题，较传统金融合约的诸要件而言(如执行条件、相关责任、抵押和担保条款、书面形式等)，网络金融服务和交易合约产生了在不同国境内的合法性问题；②若国外机构在网上涉嫌侵犯知识产权，因其认定、取证和处理难度较大，易产生相应的纠纷；③对境外信息的有效性与法律认定问题。面对非本国居民的客户时，网络银行所面临的语言选择的合法性问题。

8.3.3 网络银行对于法律风险的防范措施

针对 8.3.2 节所述可能出现的法律风险，必须采取相应的安全措施加以防范，以保障网络银行的安全顺畅运行。这是保证任何网络银行生存、发展所必须解决的问题。具体而言，对于法律风险的防范和化解可以通过以下几种手段进行。

1. 强化客户准入制度

客户资格的准入，是网络银行业务风险控制的第一道屏障。例如，银行在办理信用卡业务时，对持卡人的条件进行规定，并对其资信情况进行调查，符合条件的方可办理信用卡。再例如，中国工商银行手机银行业务管理办法规定：申请手机银行的客户，首先应当拥有中国工商银行发行的信用卡，同时必须是本地移动电话的用户。对客户资格进行限制，一方面可以掌握客户的资料，培养优质客户群体；另一方面，在一定程度上可以防止客户欺诈。

2. 明晰网络银行与客户二者之间的权利义务

对技术性较强的业务，用户办理时可能并不十分明确某些交易环节及应注意的事项。

作为交易的主体，网络银行应承担告知的义务。网络银行通常应告知如下内容：网络银行提供的服务内容、银行和用户的责任、系统安全的措施等。网络银行在与用户签约时可用书面的形式说明交易规则。说明方式必须做到公开、充分和可理解。相应地，客户在办理网络银行业务时，必须遵照银行的操作流程，支付指令应明确具体，如金额固定、收款人明确、收款人的名称和账户等正确一致、客户在网络银行的账户中有足够的款项等。接到客户的支付指令，网络银行应通过安全认证程序，严格审查、确认客户的身份及指令的真实性。对于不符合条件的支付指令，网络银行应拒绝接受并在限定时间内反馈客户不予接受之原因。网络银行对客户资料和账户交易资料有保密的义务，未经客户许可或特定执法机关依法要求，不可以将客户资料向第三方提供。

3. 确认并维护网络银行电子文件的法律效力

根据《中华人民共和国合同法》，以电子数据交换和电子邮件达成的电子合同的法律效力得以确认，并被视为合同的书面形式之一。为此，对网上银行业务的立法可以进一步确认电子合同、以纸张为载体的合同以及其他电子交易凭证、资料等在符合法定条件的情况下，具有同样的法律效力。根据我国目前有关法律的规定，计算机储存的数据资料完全可以作为视听资料类证据，但由于此类证据易于被篡改或伪造，提供方往往要负担较重的真实性举证责任。这就要求网络银行应完整保存交易原始资料，并定期将交易的计算机原始资料以对账单等形式送达客户予以确认。系统还应允许打印自己的交易记录存档，在对账单送达客户若干个工作日内，客户未向银行提出异议的，网络银行保留的电子凭证和交易记录即作为确定客户网上交易内容的有效的证据。在各项网上银行业务中，网络银行应保存好交易过程的全部电子记录，以便在纠纷中处于主动地位。银行在保全证据中，考虑到诉讼时效问题，这些资料的保存时间，按照民事诉讼法的有关规定，至少在两年以上。为了妥善保存各类电子数据信息，网络银行应该高度重视计算机及其他机器设备的运用、维护及管理，建立健全有关规章制度；并应加强员工技术培训，避免操作失误，防止因数据丢失致使银行的权利得不到法律保护。

4. 明确与网络银行高技术服务特点相适应的法律责任

由于网络银行的服务协议内容隐含了对高效率时间利用和使用便捷的承诺，客户通过网络银行进行支付交易时，责任一方对损害的赔偿不仅应包括对市场交易直接成本的赔偿，还应包括对市场交易效率成本的合理赔偿。需要明确法律责任的内容主要应包括以下几个方面。

(1) 因网络银行系统硬件出现技术故障对客户造成的损害，银行应承担民事责任，如果故障的原因应归咎于网络服务商，网络银行赔偿后可向网络服务商追索。

(2) 网络银行的安全系统是保障网络支付安全性、可靠性的重要技术系统，如果该系统出现故障或被破译，以致给客户造成损害，该安全系统的提供者及网络银行应承担连带民事责任。

(3) 网络银行内部工作人员利用工作便利，有目的地获取客户的资料，利用客户账户进行风险投资，向客户转嫁交易风险等，由此给客户造成的损害，应由网络银行向客户承担民事责任，然后再向其内部工作人员追索。

(4) 因黑客侵袭或其他网上犯罪给客户造成的损害，由于网络银行有建立安全体系、防范网上侵袭和消除网上灾难的义务，故而网络银行应对其承担责任。

阅读案例 8-4

软件设计师化身黑客，异地盗窃支付宝

重庆人李双江化身电脑“黑客”，侵入宁波一家公司的销售系统网络，利用系统数据库漏洞，侵入公司用以收款的支付宝账号，盗取资金 100 余万，最后到手 20 多万。

李双江利用系统中数据库的漏洞，使用黑客技术非法侵入，获取公司用以收款的 9 个支付宝账户，他把这些账户全都替换成自己掌握的支付宝账户。

支付宝内的钱得转到银行才能到手。李双江知道，要不被追查，就不能暴露真实身份。他通过街头办假证的广告，做了几张假身份证，办了一些银行卡。李双江用网络转账的方式，把支付宝里的钱悉数转移到银行账户中。其实，宁波的这家公司通过对账，一早知道了公司网络销售系统被侵入，对于收款支付宝被盗的事情，公司马上向宁波警方报案。

可是，盗窃对象实在难以锁定。一来，李双江远在深圳；二来，他的电脑用的是外国的服务器，警方难以确定 IP 地址。公司只能通过每天对账，了解哪些账户有款项出入，来冻结账户，让损失降到最低。

经过半年多的技术侦察，警方终于有了眉目。2009 年 7 月 19 日，宁波警方赶到深圳，在李双江租住的公寓内将他抓获。

资料来源：http://www.dxstzcy.com/index.php/news/view/id-26198.

问题：

1. 你认为上例中，造成资产丢失的主要原因是什么？支付宝公司是否需要承担一定的责任？

2. 从上例中看出，这类犯罪活动，侦察难度较大，作为使用电子支付工具的人，应该怎样加强自身资产的保护？

类似阅读案例 8-4 的案件，近年并不鲜见，不仅是专业的“黑客”会从事网络犯罪，一些具有深厚技术功底的 IT 人员在发现风险漏洞的时候，也可能难以抵挡住诱惑，最终跌入网络犯罪的深渊。一般来说，技术上的漏洞是无法完全避免的，所以如何杜绝这类犯罪显得格外困难。因此，对于公司和个人而言，要提高网络安全意识，保护自身账号的安全；对于提供支付服务的公司而言，要提高支付产品的安全机制，尽力从技术上提高安全系数；同时，对于监管机构而言，要建立起合理的法规打击网络犯罪以及明确针对这类犯罪的权责边界从而避免事后的纠纷。

(5) 如因客户遗失或泄露认证密码而造成的资金损失，应由客户自行承担。此外，还应对网络银行可以部分或全部免责的因素(如不可抗力等)进行审慎思考并做出合理规定。

5. 在合同协议中明晰各方当事人的基本法律关系

网络银行支付结算业务操作是由客户利用自己的终端或移动通信工具，通过互联网服务商，接拨网络银行业务提供商的主机或系统，通过通信系统或互联网传送到银行计算机系统，经过认证系统和网关后才能完成资金转移。鉴于这一过程中银行客户、银行、网络服务商 3 方当事人的关系比较复杂，而且我国立法对网络银行业务尚无明确的法律规定，

网络银行在开展各项业务时，必须通过协议加以规范。

(1) 用户与网络银行之间的协议。银行应针对不同的业务品种拟订有关交易当事人之间权利义务的合同规范文本，并应尽可能详尽地规定双方的具体权利义务。合同条款应重视对银行与客户之间的有关责任的分担的规定。如，约定银行对因不可抗力导致的损害免责；也可以就因供电、通信系统方面的故障所导致的损失应如何补偿等问题在协议中做出明确规定。网络银行还应在协议中对有关纠纷的解决，约定具体的方式，以促成当事人之间纠纷的迅速解决，减少损失，也可以降低纠纷对网络银行信誉的影响。

(2) 网络服务商与网络银行之间的协议。网络服务商与网络银行应在协议中明确约定，对于由网络服务系统的故障引发的有关损失，应如何处理。此外，对于系统服务商免责事项的规定，应注意与对用户承担的责任问题相连接，以避免在事故发生后，给网络银行带来不必要的损失。

(3) 硬件、软件供应商与网络银行之间的协议。网络银行与服务所需的硬件、软件供应商之间，也面临着如何承担因硬件、软件引发的事故，对客户或网络银行造成损害的责任问题。为了减少和防止纠纷发生后的争执，网络银行在购买有关硬件和软件时就应该在买卖协议中对这些事项进行约定。通过上述协议，网络银行可以将可能涉及的法律风险分摊出去，但其必须同时注意到《中华人民共和国合同法》为防止一方当事人滥用交易优势订立不合理甚至显失公平的合同，明确规定了若干限制性的条款。因此，银行在拟定合同文本时，除了分摊风险，也应当十分注重条款的公平性和合法性。

8.3.4 网络银行的监管

网络银行在带给我们种种便利、收益的同时，也引入了巨大的新风险。作为新生事物，它天生存在着合规性风险(法律风险)，即法律的空白；它的 3A(Anytime，Anywhere，Anyway)服务方式，使它更易于受到攻击，受攻击的范围更大，受攻击的方法也更加隐蔽。致使网络银行的风险和安全问题成为阻碍其自身发展的重要因素，也给网络银行的监管带来了巨大的挑战。为了实现对网络银行的有效监管，中国银行业监督管理委员会制定了《电子银行业务管理办法》，对网络的银行的监管做了变革。管理办法对金融机构开办网络银行业务的申请与变更、金融机构对电子银行业务的风险管理、金融机构利用网络银行平台与外部组织或机构相互交换电子银行业务信息和数据、网络银行业务外包管理、开办电子银行业务的金融机构利用境内的电子银行系统，向境外居民或企业提供的电子银行服务活动等内容做出了明确规定，并对银监会监督管理网络银行业务的方式与手段、金融机构违反规定应承担的法律责任等内容做出了详细规定。此管理办法是目前对网络银行业务监督管理的主要依据。但是管理办法只是对网络银行监管的一个框架性规定，对监管内容的规定大多是原则性、定性规定，缺乏具体量化内容，对网络银行交易、电子签名的法律效力及其认证等相关内容缺乏具体规定。需尽快完善相关配套制度规定。

1. 网络银行监管模式

国外对网络银行风险监管(包括对技术风险的管理)经验，比较成功的监管模式主要有美国模式和欧盟模式两种。

1) 美国网络银行监管模式

美国金融监管当局对网络银行一方面强调网络交易安全、重视银行稳健经营和对银行客户权益的保护，另一方面又认为网络银行有益于金融机构降低成本、促进服务创新，有助于实现银行间资源共享，所以不应过分干预网络银行的发展。因而，对网络银行的监管采取了审慎宽松的政策，主要通过补充金融法律法规，使原有的监管规则适应于网络电子环境要求。在监管体制、监管政策、监管内容、监管机构和监管分工等方面，美国监管当局对网络银行与传统银行要求比较相似，如大多数金融机构在开展网络银行业务时，不需要特别备案，监管当局一般通过年检收集网络银行业务数据。

目前，美国的三大主要银行业监管机构——联邦储备银行(Federal Reserve Bank，FRB)、货币监理(Office of the Comptroller of the Currency，OCC)和存款保险公司(Federal Deposit Insurance Corporation，FDIC)都把对银行业金融机构信息技术的监管作为全面风险监管的重要组成内容。

在网络银行方面，美国有如下监管措施协调：第一，制定了《计算机安全法》、《数字隐私法》、《电子商务加强法》和《银行用户身份认证体系》等法规，实施了 ISO/IEC15408-1999 和 ISO17799-2000 等信息安全国际标准；第二，监管内容制度化、规范化，美国联邦金融机构检查委员会(FFIEC)颁布了一整套信息技术检查手册，共涉及 12 个方面的内容，对监管者、银行机构和信息技术提供商应关注的风险及如何识别、分析、预警和控制，提出了明确的指导意见；第三，银行业监管信息化与银行业金融机构的信息化同步推进，并做到监管机构之间信息共享；第四，监管方式多样化，包括现场检查、非现场分析和评级、技术提供商准入管理、发布 IT 技术规章和指导、推动外部评级和审计、IT 风险信息披露等多种手段。

和其他国家的做法一样，美国也将巴塞尔委员会对网络银行风险管理本土化，并制定出其基本程序。例如美国通货监管局负责监管美国的国民银行，随着大量国民银行采用各种各样的电子技术，向客户提供网络银行的服务，国民银行将与技术有关的风险管理分成了计划、实施、检测和监控 4 个步骤。

2) 欧盟网络银行的监管模式

欧盟对网络银行监管所采取的办法较新，其监管目标主要有两点：第一，提供清晰、透明的法律环境；第二，坚持适度审慎和保护消费者的原则。与电子银行有关的法律法规包括《电子商务指导》、《远程销售金融服务指导》、《布鲁塞尔公约》和《罗马公约》等。欧洲中央银行要求其成员国采取一致性的监管原则，欧盟各国国内的监管机构负责监管统一标准的实施。它要求成员国对网上银行业务的监管保持一致，承担认可电子交易合同的义务，并将建立在“注册国和业务发生国”基础上的监管规则，替换为“起始国”规则，以达到增强监管合作、提高监管效率和适时监控网络银行风险的目的。

欧盟对网络银行的监管主要集中在以下几个方面：①区域问题，包括银行业的合并与联合、跨境交易活动等；②安全问题，包括错误操作和数据处理产生的风险、网络被攻击等；③服务的技术问题；④随着业务数量和范围的扩大而增加的信誉与法律风险问题。

2. 我国网络银行法律监管问题

首先，监管目标缺乏对客户利益的维护。我国 2001 年颁布的《网上银行业务管理暂

行办法》第一条就规定了我国网络银行的监管目标：第一，规范和引导我国网络银行业务健康发展；第二，有效防范银行业务经营风险；第三，要保护银行客户的合法权益。可见，处于首要位置的是网络银行业的发展而非维护客户的利益。当两者发生冲突时，客户利益就要服从于行业利益的需要，使客户蒙受一定的经济损失。一方面，网络银行的服务协议中的相关条款在加重了客户责任的同时减轻了自己的责任。具体来说，现在的网络银行一般都会与客户签订一份“网络银行服务协议”，假如不同意该协议则无法申请或开通网络银行。一旦客户开始正式申请网络银行服务，就被视作接受了服务协议的所有内容，或由客户领取的服务协议经客户和银行签字确认生效。这样的“服务协议”从内容上看，包含了一般合同所具有的内容，其性质是明确客户及银行双方的权利义务的合同。客户如果希望获得银行的网络银行服务，只能简单地表示接受却不能提出修改条款的具体内容。根据我国《合同法》第三十九条“格式条款是当事人为了重复使用而预先拟定，并在订立合同时未与对方协商的条款。”可见，现在所有由银行提供的“服务协议”的内容都是格式条款，对于提供格式条款的一方除了应遵循公平原则确定当事人之间的权利义务关系，在对该条款进行说明的义务外，还要承担《合同法》第四十一条规定的：“对格式条款有两种以上解释的，应当做出不利于提供格式条款一方的解释”的风险。另外，根据《合同法》第四十条：“提供格式条款一方免除其责任、加重对方责任、排除对方主要权利的，该条款无效。”但实际情况却是许多已经建立的网络银行以及正在筹建的网络银行的服务协议中有关条款加重客户的责任而减轻自己的责任。一旦发生与客户的纠纷，这些由银行精心制定的条款，便不能及时有效地保护客户的利益或存在不能保护客户方利益的风险。

另一方面，将不可抗力作为网络银行的免责条款的规定，显得过于空泛，缺乏对客户利益的保护。在所有的网络银行服务协议中都约定了遇到不可抗力而发生意外事件时，银行可以不承担任何责任。这样的协议从法律角度来看是不合理的。根据《合同法》规定，应不可抗力不能履行合同的，根据不可抗力的影响部分或者全部免除责任。即在发生不可抗力的情况下，不能履约的一方并不一定能够全部地免除履约责任，需要根据不可抗力的实际影响，在受影响的实际范围内方可免除责任。同时，服务协议中所称之不可抗力均未有具体说明。因此，在网络银行业务这种的新型服务模式中，可能出现种种的意外事件，如银行系统遭黑客攻击等。在这些情况下，假如银行能够举证对自身系统采取了应尽的防范义务，仍然无法阻止该事件案发生，则可以视为发生了不可抗力；反之则不能。又根据《合同法》的规定：“当事人一方因不可抗力不能履行合同的，应当及时通知对方，以减轻可能给对方造成的损失，并应当在合理的期限内提供证明。”当事故出现后，银行应尽及时通知客户的义务。银行应该对经营网络银行业务过程中可能发生的无法正确执行客户指令的情况进行预测与分析，将可以视为不可抗力的情形归入免责条款，约定提供证明的内容和期限以及及时通知对方的义务。

其次，网络银行监管法律体系不完善。我国的网络银行监管法律体系尚处于起步阶段，关于网络银行监管的相关法律几乎处于空白状态。目前，在法律层次上主要包括《银行业监督管理法》、《中国人民银行法》和《商业银行法》的规定。作为信息技术的一种应用，网络银行还要遵守《安全法》、《保密法》与刑法中有关计算机犯罪的条款。但总体说来，相关的专门性法规依然缺乏：①电子化交易的基础法制欠缺。我国虽然通过了《电子签名

法》，但与国外的相关立法比较，目前我国的这部《电子签名法》在电子合同、电子商务消费者保护与电子商务经营者的法律责任等领域依然有所欠缺；②《商业银行法》、《人民银行法》及人民银行的金融规章均无针对网络银行业务的专门规定，现有的银行监管法制均未对网上银行业务的进入及具体业务开展进行规定，使得监管机构的监管“无法可依”，为此，网络银行交易的高风险性要求国家有必要对网络银行业务进行行之有效的监管；③对于利用网络银行进行犯罪的行为，我国刑法缺乏具有针对性的处罚条款，针对利用网络银行洗钱的犯罪问题、伪造、复制电子货币的犯罪问题、对网络银行的系统侵袭攻击行为的犯罪，我国刑法中的定罪量刑条款依然缺乏，难以有效的对其进行打击和惩处。

此外，在网上银行的法律监管方面仍然存在如机构型监管体制导致网络银行监管出现真空，市场准入监管制度存在弊端，外部监督影响网络银行监管的效率等问题。总之，我国目前实行的网络银行监管法律制度是不甚完善，急需借鉴国际先进经验，对网络银行监管制度进行有效改革，构筑相应的法律制度。

3. 我国网络银行监管的应对措施

面对现存的诸多问题，如若不对网络银行的监管及时进行调整与完善，势必有碍于我国新型金融服务的进步，不利于我国市场经济的健康持续发展。有鉴于此，网络银行监管制度完善的重要作用就更加凸现出来了。在完善我国网络银行的监管过程中可以从以下两个角度来考量。

(1) 完善客户利益保护制度。首先，应为客户提供解决问题的替代方式及投诉程序。由于网络银行可能会出现各种不可预期的问题，所以银行应提供有效的技术性支持，如列明银行的有效联系电话、银行的投诉处理程序及对争议解决程序制定相关应急机制以应对各种问题。其次，应提供审查要约或承诺内容的机会。美国《信息交易法》第 112 条第 5 款第(a)项规定：“电子代理人应该提供条款审查机会”，“只有在以一种必定能引起正常人的注意，并允许其审查的方式，才能使某人能利用该审查记录或条款。”此条款值得我们借鉴。再次，应明确银行的赔偿责任，明确银行与客户之间的权利义务。目前，国际上已有一些规则对银行网络的赔偿责任加以规范，如国际贸易法委员会国际支付小组 1992 年起草的《国际资金划拨标准草案》与美国 1989 年的《统一商法典》中都有关于银行延迟执行、不适当执行及没有执行其应执行的支付命令的，其损失赔偿责任仅限于划拨的费用及被划拨的利息，除非有明示的书面协议，否则不对用户的间接损失负责的相关规定。因此，一方面我们可以采用以优先责任原则为主，兼采用完全责任原则的方法。若网络银行因疏忽迟送、误发支付信息的，其赔偿责任限于传递费或支付命令金额加利息，除非事先预见到会发生这种损失；若故意或欺诈性地泄露用户商业秘密或更改、损毁用户交易数据的，其赔偿额应为用户的全部损失；假如起因于银行有义务维护网络通信的先进性等方面的问题，银行对此应负赔偿责任；但因突发性停电或人为破坏网络等，银行则不需负赔偿责任等。另一方面，制定有关赔偿责任的强制性法规以解决网络银行与用户的责任问题。在目前尚无法律规范的情况下，用户与网络银行必须就相关问题达成协议，明确双方法律责任。

(2) 完善我国网络银行监管的法律体系。制定一部实体法与程序法相结合的网络银行监管法，既要规定网络银行监管目标、监管原则、监管机构等实体法律问题，也要规定网

络银行的基本诉讼程序问题。但该法对上述内容仅应作原则性的规定，以尽可能避免法律的滞后性所带来的问题。另外，还需制定与之相配套的网络银行管理办法的实施细则。这样的实施细则可以将网络银行监管中的许多具体问题予以规定、细化。还可以参照美国制定指引公告，对网络银行的技术管理和风险管理作出规定，对监管当局目前已经认定但未成熟的技术操作系统、风险管理手段或那些如不加以适当的管理，就有可能形成系统性风险的业务流程、项目检查手段等加以公布，并随着情况的发展变化而不断的予以调整。

此外，从我国实际情况出发，应采取三位一体的监管模式，将政府监管、银行行业协会自律管理与银行内部控制三者相结合，完善我国网络银行的监管。

市场经济是法制经济，在网络经济条件下诞生的网络银行也离不开法制的保障和支持，应积极建立适应于网络经济条件，推动网络金融发展的监管法规体系。

对于之前提到的央视曝光的现象是可以避免的，用户只需做到以下 3 点便可保证网上银行的安全。

(1) 登录正确的银行网站:直接输入银行网址，而不是从不熟悉的邮件或网站链接进去。

(2) 保护电脑安全:安装防病毒软件，并及时更新病毒库。中国金融认证中心也已经在许多银行的网站上免费为用户提供“网银病毒专杀工具”，专门针对盗取网银信息的木马病毒。

(3) 保护密码，正确使用数字证书:保护密码大家比较熟悉，这里重点介绍保护数字证书。证书可以存放在电脑里，也可以存放在硬件介质 USBkey 里。如果存放在电脑里，就要保护电脑安全。中国金融认证中心免费向大众提供的“证书保险箱”，就是专门用于保护存放在电脑中的证书的。如果存放在 USBkey 里，注意使用后要及时拔出。

面对“黑客袭击”，广东工行和农行都已做出回应。广东工行建议，客户对自己的电脑系统做一些必要的安全管理，可以极大地降低黑客访问的概率。该行推荐客户使用 Windows 2000(SP4)、IE 6.0(SP1)以上版本的操作系统，并定期下载安装最新的操作系统和浏览器安全程序或补丁。此外，广东工行提议选择必要的安全工具包括 U 盾、口令卡，以及余额变动提醒、手机短信认证、预留验证信息、小 e 安全检测等服务。而广东农行对于个人注册用户已经实现中国银监会提出双重身份认证的措施。目前，农行个人注册用户使用的网上银行证书有两种模式，分别是 IE 浏览器证书和附有物理介质的网上银行 KEY 证书。除了使用介质数字证书作为有效的安全保障措施外，农行网上银行系统还采用了防火墙、入侵检测等多种安全措施，能够有效阻止来自互联网上的各种网络攻击，而进行转账交易所使用的图形码和密码键盘是防范风险的另一种有效保障措施。

另外，在全国两会上通过的《刑法修正案(七)》，明确提出要对木马病毒罪行进行严惩。这说明网络盗取用户各类账号信息的打击行动，今后将得到法律支持，钓鱼网站进行欺骗等不法手段也将受到法律的威慑；同时，整治木马病毒“黑色产业链”从此将有法可依，凡是提供工具、程序以用来入侵、控制和非法获取信息的行为将难逃法律惩罚。

8.4 第三方支付的法规和监管

阅读案例 8-5

网络虚拟资产案件首次采取诉前保全措施

2008 年 2 月 20 日，原告上海一家广告公司聚和堂因一起委托买卖合同经济纠纷与被告另外一家网上服装销售公司在法院的主持下当庭交换了证据。随后，上海聚和堂广告有限公司申请诉前对被告在互联网支付平台——“支付宝”内的 50 多万元财产执行保全措施。由于网络交易支付方式有别于传统市场交易支付方式，所以上海一中院对该起涉及网络虚拟资产的保全案件进行了充分研究，并制定了完整的执行方案。执行人员随即奔赴互联网“支付宝”在杭州的总部，通过该部人员的协助，成功冻结了被告在互联网上以虚拟账户登录名和号码开设的交易账户内资产。

在 2008 年 12 月 25 日召开的“首届电子支付业务与创新发展研讨会”上，中国人民银行支付结算司司长欧阳卫民表示，要尽快建立规范第三方支付平台的发展制度。据悉，央行正在研究电子支付二号令，这是专门针对第三方支付平台的支付指引。

调查机构易观国际最新报告显示，2008 年第三季度，国内第三方支付市场交易额总规模达到 661.99 亿元，比上一季度增长 23%。除了在网上零售市场，第三方支付在电子机票市场、B2B 市场以及电信、金融等细分市场都有明显增长。调查机构分析普遍认为，目前第三方支付已经成为互联网的一项基础应用，在人们的生活中发挥了日益重要的作用，不过部分业内公司存在的风险管理、恶性价格竞争等问题也日益突出。由此可见第三方支付法规和监管的重要性。

资料来源：http://tech.163.com/08/0225/08/45HLKQSG000915BF.html.

问题：

1. 通过上例，你认为第三方支付会产生哪些法律问题？
2. 监管机构应采取哪些措施从而加强对第三方支付的监管？

阅读案例 8-5 中，此次被冻结款项案件的诉因可能是某公司因拖欠广告费被一家广告公司申请冻结的账户。但从维权的角度看，此次冻结对于打击利用淘宝网等 C2C 平台进行侵权行为的影响非常深远。

在以往，维权者在类似淘宝、易趣和拍拍之类的交易平台上发现了出售侵权产品的网页后，无论其是通过向交易平台发函要求其删除相关出售侵权产品的网页，还是直接起诉交易平台运营商侵权，效果都不太好。如果要求交易平台删除网页的，侵权者可以马上另行发布侵权产品销售网页。而起诉交易销售平台的，即使在知识产权保护力度很大的美国，维权者胜诉的难度也很大，在处于社会主义初级阶段、知识产权保护力度不如美国的中国就更难了。

而现在，如果维权者通过诉讼对交易平台上出现的一些侵权行为者进行起诉，同时依据相关的法律向法院申请对其支付宝或者类似账户进行冻结，将会对侵权者产生较大的影响。

首先，此类诉讼的证据收集比较便利，淘宝网等 C2C 网站都可以通过信用查询方式查到卖家近半年的交易记录，也就是说侵权行为记录有据可查。对于维权者的诉讼胜诉较为有利。

其次，对于被诉者而言，还存在淘宝账户信用度的损失，一旦支付宝账户被冻结，其相关联的淘宝卖家账户也只能随之废弃，否则在此账户销售产品的货款将可能都被冻结。鉴于 C2C 交易的特点，卖家账户的高信用度对于销售的促进作用比较大，能通过诉讼迫使其放弃账户加大其侵权成本。

第三方支付在我国获得了突飞猛进的发展，其市场空前壮大，参与其中的商家和消费者规模越来越大，不可避免地要面对这个市场上存在的各种关系，尤其是法律关系。法律关系是维系这个市场井然有序的基础，也是其他关系的基础。当然，第三方支付中的法律关系源自传统支付中的法律关系，却有其独特性。

8.4.1 第三方支付的法律关系

第三方支付的法律关系主要涉及两种法律关系：一是民事法律关系，主要是买卖双方和第三方支付机构之间的法律关系，从性质上说属于民事法律关系；二是行政法律关系，即国家为规范第三方支付行为制定相应的监管法规，监管机关依据这些法律法规对第三方支付机构的活动进行监管形成的法律关系，其性质上应当属于行政法律关系。

民事法律关系主要涉及两个方面。以买卖关系为例，以资金的支付为媒介，买卖双方都要和第三方支付机构发生法律关系，即买方(付款方)和第三方支付机构之间的法律关系，第三方支付机构与接受付款的电子商务企业(收款人、卖方)之间的法律关系。这些关系大致可以归入民法领域的委托代理关系，买方和第三方支付机构之间的法律关系还有资金保管关系，即在买方确认支付之前，买方的资金是由第三方支付机构代为保管的，由此在买方和第三方支付企业之间构成了资金保管关系。总之，第三方支付机构自身不是银行，其向用户提供的服务是支付处理服务，而不是银行业务；对于用户的资金，第三方支付机构不是财产的受托人、受信托人或者是待一定条件成熟后再转交给受让人的第三方，而是作为用户的代理人和资金的管理者。第三方支付机构与用户形成的委托代理法律关系，主要是通过第三方支付机构制定的格式合同来加以规范和调整的。

除此之外，第三方支付机构和银行之间因为资金往来而形成了相应的法律关系，这些法律关系也主要由民法加以调整和规范，从而形成民事法律关系。第三方支付机构与银行之间签订有关协议，使得第三方支付机构与银行可以进行某种形式的数据交换和相关信息确认。这样第三方支付机构就能实现在持卡人或消费者(买方)与各个银行，以及最终的收款人或者是商家(卖方)之间建立一个支付的流程。

行政法律关系主要是指监管机构与第三方支付机构之间的关系。在法律上明确二者之间是监管与被监管的关系，制定相应的监管细则，例如对明确第三方机构的身份认证程序以及建立市场准入机制、第三方支付机构资金管理、风险控制等。监管机构是保证第三方支付机构健康发展和保护消费者权益的关键，因此，从法律上规定二者之间的权责尤为重要。

8.4.2 第三方支付的潜在问题和风险

第三方支付的功能就是为电子商务网站的交易者，以及其他网络交易的双方乃至线下交易者提供“代收代付的中介服务”或“第三方担保”。正是由于第三方支付公司处于这种中间人的地位，使得第三方支付存在着潜在的问题和风险。

1. 第三方支付公司的法律地位不明确，缺乏相应准入监管

作为支付中介的第三方支付公司，处于网络运营与金融业务交接的“灰色地带”。通常而言，如果不是仅仅提供技术平台，支付中介服务(特别是非监管型账户支付模式的第三方支付公司提供的网上账户资金转移服务) 实质上类似于结算业务，而结算业务，根据我国《商业银行法》的规定属于商业银行的中间业务，必须经过银监会的批准才能从事。在国内，法律规定只有金融机构才有权利吸纳代理用户的资金，其他企业和机构不得从事类似的活动。但由于第三方支付平台出现不久，所以目前还没有相应金融监管法规和机构管理。

2. 第三方支付公司从事资金吸储并形成资金沉淀

(1) 第三方支付平台利用资金的暂时停留，在交易过程中约束和监督了买家和卖家。但是，不能忽视这样一个事实：当买方把资金划入第三方的账户，第三方就将起到了资金保管人的作用。资金的所有权并没有发生转移，买方仍然是资金的所有人，当买方和卖方达成某笔交易，买方收到商品，通过第三方向卖方付款时，此时款项的所有权应仍属于买方所有，直至款项进入卖方账户，或者卖方确认接受付款后，所有权转为卖家。可以看到，第三方作为款项的保管人，始终不具备对资金的所有权，只是保管的义务。随着将来用户数量的增长，这个资金沉淀量将会非常巨大。根据结算周期不同，第三方支付公司将可以取得一笔定期存款或短期存款的利息，而利息的分配就成为一大问题。

(2) 第三方支付平台中的大量资金沉淀，如缺乏有效的流动性管理，则可能存在资金安全，并可能引发支付风险和道德风险。除支付宝等少数几个支付平台不直接经手和管理来往资金，而是将其存在专用账户外，其他公司大多代行银行职能，可直接支配交易款项，这就可能出现非法占用和挪用往来资金、不受有关部门的监管，而越权调用交易资金的风险。

3. 第三方支付平台面临着网络违法犯罪活动的风险

(1) 由于网络交易的匿名性、隐蔽性，第三方支付平台很难辨别资金的真实来源和去向，使资金的非法转移、洗钱、贿赂、变相侵占国有资产、收受回扣、诈骗等活动有了可乘之机。

(2) 利用第三方支付平台进行信用卡套现，规避相关的利息费用，无偿占用银行信用资金。

(3) 为规避银行汇划手续费，通过创建虚假交易将资金从 A 的支付平台账户转至 B 银行账户，再提取资金至指定银行卡账户。

(4) 成为网络赌博的又一渠道，如 2006 年德国世界杯足球赛期间，可疑交易有上升趋势。

(5) 利用目前工商、税务的漏洞，企业以个人名义进行交易，逃避税收，形成税收黑洞。

4. 第三方支付市场的消费者保护问题

第三方支付公司在经过一段时间的无序竞争后，不可避免地开始进行洗牌、兼并、重组、并购、转型等。如果在第三方支付公司面临可能的暂停或者关闭时，作为用户的资金如何得到保全并退偿，将是一个严肃的问题。目前，作为接受第三方服务的消费者，面对可能的经营和政策风险缺少一个强有力的保护。此外，当第三方支付公司终止服务时，支付平台的账号、账号中的资料和档案如何受到保护，也没有明确的监管要求。网络支付无论从其系统设计还是业务流程来看都比现金或其他非现金支付方式复杂，对消费者的行为要求也相对较高，为避免网络支付中介利用这种信息技术和业务上的优势损害消费者利益，必须强调对消费者的利益保护，以维护交易公平。

对于保留客户个人支付资料(卡号、姓名等) 的第三方支付平台，还存在着网上消费者个人资料泄露的风险，一旦用户的个人资料被泄露，将造成很大的金融损失。因此，如何规范第三方支付平台的消费者支付信息保护也是很紧迫的问题。

阅读案例 8-6

卡付通网站突然关闭：消费者蒙受损失

2009 年 7 月，一个声称免收手续费帮助用户信用卡还款和转账的卡付通网站突然关闭了。这是国内首例第三方支付网站携款逃跑事件，已有 60 多人声称因使用卡付通网站损失了钱财，受害者来自全国各地，涉及广东、江苏、浙江、山东等近 20 个省份和地区，怀疑损失的金额大约近 20 万元。这些用户为什么会在网上使用卡付通网站付款？据了解，是因为网民在通过卡付通网站付款的时候，出现了国内公认信用度和知名度很高的独立第三方支付平台支付宝网站的页面。

随着我国电子商务的蓬勃发展以及网上购物人群的迅猛增长，我国的电子商务市场在信息流、物流等方面的大部分难题已经得以解决，然而支付问题却成为了如今制约我国电子商务发展的瓶颈。随着网民对网络支付形式接受度的提高，更多的商家开始将网络支付作为自己业务的一种支付方式提供给消费者。“支付宝”、“ 财付通”等第三方支付工具以及赔付制度更是在很大程度上改善了电子商务的购买信任危机，第三方支付方式借着网络支付市场的“东风”得以迅速的发展。据统计，除阿里巴巴的“支付宝”和 eBay 的“贝宝”外，目前中国市场上有 50 余家中小规模的第三方支付公司，根据赛迪顾问的分析，2005 年、2006 年网络支付和移动支付的第三方支付业务分别为 179 亿元和 242 亿元，同时，2007 年中国第三方网络支付业务规模已超过 280 亿元，占网络支付市场规模的比例达 36%左右。这说明第三方支付在网络支付中已经扮演着越来越重要的角色，所以第三方支付的规范和监管问题也随之备受关注。

资料来源：http://www.donews.com/Content/200907/0e19a678-5b3c-4f27-9108-e412b4043bed.shtm.

问题：

1. 是否应该加强对第三方支付网站的资格审核，为什么？
2. 你认为，审核第三方支付网站的资格，应制定哪些标准？

从阅读案例 8-6 看出，第三方支付是一个巨大的市场，越来越多的商家想进入该市场。虽然，更多的第三方支付平台，会对这个市场的繁荣有助益，但政府却不能忽视对第三方支付平台准入资格的审核，建立起完善的监管机制是当前要解决的首要问题。

8.4.3 现有第三方支付的监管情况

关于第三方支付的监管问题，是现在讨论的热点，也是政府机构和相关组织极为关注的问题。

阅读案例 8-7

马蔚华呼吁加强监管不达标第三方支付企业

2009 年 3 月 6 日，全国政协委员，招商银行行长马蔚华近日提出提案指出，第三方支付企业运作管理水平参差不齐，建立牌照发放制度，有利于产业集中，使不达标的中小支付企业自动退出市场。

马蔚华认为，第三方支付平台通过虚拟账户和在途资金，沉淀了大量客户资金，第三方支付企业可将这些资金用于风险较高的投资活动或其他活动，加上各企业运作管理水平不一，可能引发流动性风险、信用风险和操作风险。此前一些支付平台交易的匿名性、隐蔽性以及信息的不完备性也可能增加风险。

马蔚华还提到，要加强第三方支付平台的用户沉淀资金的管理，必须实行用户资金(包括虚拟账户余额及在途资金)与企业的运营资金分离，由银行进行专户监管，保证在途资金的安全和不被挪用。其次，对于第三方支付平台中资金的转移，也可增加银行审核环节，在一定程度上消除洗钱等安全隐患。最后，第三方支付平台账户运营及管理应比照银行账户的监管要求。

同时，马蔚华强调，国家应该尽早出台《支付清算组织管理办法》等规范第三方支付平台经营行为的相关法律法规，规范第三方支付平台业务范围，消除“灰色地带”。

资料来源：http://www.donews.com/Content/200903/aa3df7c2-55dc-4abb-84f1-0530d32a3f22.shtm.

问题:

1. 对于本案例，你是否赞同马蔚华的对第三方支付的提案？并给出理由。
2. 结合你所学的知识和本案例内容，分析目前我国对第三方支付的监管状况？
3. 你认为国家应该如何在法律法规方面加强对第三方支付的监管？

阅读案例 8-7 中招商银行行长马蔚华从三个层面上提到对第三支付平台的监管，然而，在建立监管机制之前，监管机构应深入剖析国外的监管实践，同时结合国内的环境，进而制定出完备和行之有效的监管体系。

1. 美国对第三方支付平台的监管状况

第三方网络支付平台的发源地是美国，因此，在对第三方支付的金融监管上，美国也走在前面。

(1) 在法律方面，美国在现有的法规中寻求相关的监管依据，或对已有的法规进行相应的增补，没有制定针对第三方网络支付平台的专门法规条例。

(2) 在监管体制上，美国采用立体的监管体制，从联邦和州两个层面对第三方网络支付平台进行监管，将监管的重点放在交易的过程，而不是从事第三方支付的机构，其中，美国联邦存款保险公司(FDIC)是监管的重要部门。

(3) 在对第三方支付平台的身份划分上，美国联邦存款保险公司(FDIC)把第三方网络支

付平台上的滞留资金定义为负债，而不是联邦银行法中定义的存款，这样第三方支付平台就不能被划分为银行或其他类型的存款机构，从而不需获得银行业务许可证。

但 FDIC 同时指出，各州监管部门可依据本州法律，对第三方网络支付平台开展的业务做出自己的定位。目前，美国大多数州为该平台颁发了从事货币转账业务的营业许可证，并要求其定期向州监管机构提交报告，并规定了最低的资本要求，将客户资金的投资限定在高流动性的范围。美国监管机构在监管方式上采取了现场检查和非现场检查相结合的方式。

(4) 在对第三方支付平台滞留资金的监管上，FDIC 通过提供存款延伸保险实现对滞留资金的监管。FDIC 规定每个第三方网络支付平台都必须在 FDIC 的银行中开一个无息账户，该平台的滞留资金必须及时的存放在相应的账户中去。并规定每个用户账户的保险上限为 10 万美元，保险费由这些滞留资金也就是客户资金在银行产生的利息来交纳，一方面，避免了第三方支付平台人为的延长在途资金的在途时间问题，解决了平台和用户之间的利息分配问题，另一方面，当该支付平台资金出现问题时，可以用保险金来降低客户的损失。其次，FDIC 严格规定第三方支付平台只是客户资金的代理人，将客户账户和公司账户分开，无权将客户资金进行贷款，移作公司经营之用，或在公司破产时用于清偿债务。

(5) 在对非法金融活动的监管上，美国颁布了《爱国者法案》，规定第三方网络支付平台作为货币服务企业，需要在美国财政部的金融犯罪执行网络注册，接受联邦和州两级的反洗钱监管，及时汇报可疑交易，保存所有交易记录。

(6) 在对电子货币的监管上，美国 50 个州中有 43 个州以及哥伦比亚特区对非银行的电子货币发行方进行了监管，但没有专门的电子货币监管法规，而是依照已有的(或增补的)监管货币转移企业或者货币服务企业的州法律进行监管。由于各个州的执照相互不被承认，第三方网络支付服务商需要分别取得当地的货币转移企业和货币服务企业营业执照才可发行电子货币。由于美国的监管体系较少涉及资本金要求，因此进入门槛相对较低。在联邦层次上，美国近年来也开始关注电子货币的监管，尤其在对消费者的保护方面，《银行安全法案》的许多规定也被运用于对第三方网络支付平台的监管。

2. 欧盟对第三方支付平台的监管状况

与美国相比，欧盟在对第三方支付的监管上有自己的特点。

(1) 在对第三方支付平台的身份划分上，欧盟规定网上第三方支付的介质只能是商业银行货币或电子货币，这就意味着第三方网络支付公司必须取得银行业执照或电子货币公司的执照才能开展业务。

(2) 在法律法规上，欧盟出台了专门的监管的法律框架，主要有 3 个指引文件，通过对电子货币的监管来实现对第三方网络支付公司的监管。2000 年 1 月颁布了《电子签名共同框架指引》，在该指引文件中确认了电子签名的法律有效性和在欧盟内的通用性。同年又颁布了《电子货币指引》和《电子货币机构指引》两个指引文件，要求非银行的电子支付服务商必须取得与金融部门有关的营业执照(完全银行业执照、有限银行业执照或电子货币机构执照)。

(3) 在对第三方支付平台滞留资金的监管上，欧盟规定第三方支付平台需在中央银行开设专门的账户留存大量资金，并将电子货币的发行权限定在传统的信用机构和新型的受监管的电子货币机构。对于增值服务，目前还没有适用于整个欧盟的法律法规。由于欧盟致力于

建设单一欧盟支付区(SEPA)，第三方支付公司只要取得 “单一执照”，便可在整个欧盟 25 国通用。例如，PayPal 在 2004 年取得了英国金融服务局(Financial Services Authority，FSA)颁发的电子货币机构许可证，并接受 FSA 的监管，就可以在欧盟其他成员国开展业务。

(4) 在对电子货币的监管上，欧盟规定机构和个人也可以发行货币，但需要通过相应的审批、获得执照，如在英国由金融服务业协会向希望发行自己货币的公司发行许可证并进行监管，比如说规定发行额不能超过 5 万欧元。英国一些公司已经拿到了合格证，包括一些大学在内。

(5) 在对非法金融活动的监管上，与美国一样，实行审慎的监管，限制将客户资金用于投资，反洗钱等。

3. 亚洲对第三方支付的监管状况

第三方网络支付平台在亚洲的出现较欧美略晚，仍处于发展初期，但各国(地区)政府一直密切关注其发展，不断调整相应的监管措施。

新加坡在 1998 年就颁布了《电子签名法》。韩国在亚洲金融危机后成立了新的金融监管委员会(FSC)，于 1999 年颁布《电子签名法》。中国香港则在 2000 年颁布《电子交易法令》，给予电子交易中的电子纪录和数字签名与纸质对应物同等的法律地位，并增补了有关电子货币发行的法律。另外，香港金融管理局还采取了行业自律的监管方式，收到了较好的效果。

中国台湾对网络支付中使用电子支票的监管给予了较多重视，颁布了《电子商务中的电子签名法》、《从事电子支票交换的金融机构管理条例》以及《申请电子支票的标准合同》等等。但是，各国(地区)目前都没有对第三方网络支付平台制订专门的监管法规，相应的监管政策仍处在探索阶段。

8.4.4 我国第三方支付监管现状及监管趋势

1. 现状

我国大陆还没有出台专门针对第三方支付的法律法规，可以依据的只有“三个参考”，即一条法律、一条指引、一个办法。2005 年 4 月 1 日起施行的《电子签名法》规定可靠的电子签名与手写签名或者盖章具有同等的法律效力，从而在法律层面上规范了网络支付中的电子签名行为。同年 10 月 26 日央行针对电子支付的首个行政规定——《电子支付指引(第一号)》正式实施。2005 年 6 月 10 日，中国人民银行发布了《支付清算组织管理办法》(征求意见稿)(以下简称《办法》)，对从事网络支付业务的非银行机构的性质、业务开办资质、注册资本金、审批程序、机构风险监控以及组织人事等做出了相应规定。

随着《办法》的出台，中央银行通过发放经营资格牌照的政策来提高第三方支付公司的门槛。这一措施有利于解决现有的盲目扩张现象，整合优良资源。同时，实力较弱的公司将面临被收购和兼并的可能，建立完善的市场退出机制，有利于保护客户利益。

此外，目前工商银行要求第三方网络支付公司要将上个月交易总额的 30%滞留在该公司在工行的保证金账户。如果该企业要停业，工行方面将立刻对外发布公告。这种措施有利于保障交易支付资金的安全，防范第三方网络支付平台的支付风险和信用风险。

2. 监管趋势

目前我国相关的专门规范还比较缺失，使得第三方支付机构游离于监管之外，从而不利于我国的金融安全。存在主要问题有：相关监管法规欠缺；第三方支付的安全问题；第三方支付的税收问题等。针对上述监管的缺位，我国第三方支付的监管呈现以下趋势。

1) 尽快明确第三方网络支付公司的法律身份

《办法》提出第三方网络支付结算属于支付清算组织提供的非银行类金融业务，第三方支付公司是金融增值业务服务商，这样的定位符合我国现有国情，物理上掌握或控制现金流不是判断是否是银行的标准，第三方支付公司只是银行业务的补充和延伸。

2) 建立市场准入机制

建立完善的市场准入机制，包括设置最低资本金限制，加强内控机制和风险管理，强化安全技术、建立保险与保证金问题。关于资本金的限制，《办法》中虽已列出，但还不能具体操作。目前我国在内控机制和风险管理方面不管是网络银行还是电子支付都还没有相应的法律规定。在安全技术要求方面，除准入控制外，建立完备的基础设施以确保客户交易活动安全性和交易记录的真实性非常必要，可以考虑借鉴欧盟的一些做法，在我国《电子银行安全评估指引》基础上对电子支付做出规范。对非金融机构采用类金融机构设置保证金机制，并积极研究电子支付保险问题。

3) 加强对滞留资金的监督和管理

对滞留在第三支付公司内部的客户资金，通过法规明确其所有权属于客户，严格区分客户的资金和第三方支付公司自身的资金，采取类似证券交易保证金账户的监管要求，要求实行银行专户存放和定向流动。禁止将客户资金用于第三方支付公司运营或者其他目的，明确第三方支付公司在破产等退出市场的情况下对客户资金的保全责任。

4) 明确商业银行的代位监管

通过立法明确商业银行在第三方支付市场中的代位监管义务，即对于第三方支付公司开立在银行的支付结算专户，商业银行必须履行相关监管规定，监控该账户的资金流动情况，确保资金的合法使用。

5) 加强对消费者的利益保护

通过立法加强对消费者的利益保护，避免非银行机构利用信息和技术、业务上的优势损害消费者利益，维护交易公平，确保数据保密和信息安全。

6) 完善担保及税控体系

由于第三方支付市场的发展尚处于初级阶段，为了增强信用及风险防控体系，可以通过尝试建立金融担保制度来防范和化解风险。同时在税收方面，加快研究制定电子商务税费优惠的财税政策，可参照国外对电子商务企业征收税费的优惠措施，实行“前几年免，后几年减半”的办法。相应的税收优惠政策应将第三方支付主体囊括在内，在扶持和规范产业发展的同时，减少偷税漏税的违法行为。

8.5 第三方认证中心的法规和监管

8.5.1 电子认证中的法律关系分析

1. 认证机构与电子签名人之间的法律关系

在电子交易中，签名人需要利用电子签名来证明自己的身份并保障数据的安全传输，认证机构提供证书服务，目的是表明电子签名人身份信息的真实性，使其电子签名能为他人所认可，同时也可了解其他签名人的真实身份，增加交易机会，促进交易成功。认证机构提供的证书服务是一种信息服务，认证机构与电子签名人之间通过认证证书联系起来，认证证书是认证服务合同的格式化体现，两者之间应属合同关系。

在电子认证活动中，电子签名人需向认证机构提交内容完整的申请书，提供必要的信息资料和证明文件，该过程可看作为电子签名人向认证机构发出要约；认证机构受理申请后，应遵循相关规定及程序对申请者的身份及提供的信息进行审核鉴定，经审验，如申请人提供的信息真实、完整和准确，则可批准向申请者签发认证证书，即认证机构做出承诺，申请人成为证书用户，两者之间合同关系成立。认证证书的签发、对证书生命周期内的有效管理及收取相关费用，都应视为合同的履行行为。我国《电子认证管理办法》第二十二条规定：“电子认证服务机构受理电子签名认证申请后，应当与证书申请人签订合同，明确双方的权利义务。”由于电子认证服务的特殊性，法律对认证机构和电子签名人的权利义务设定了很多强制性条款，对两者之间的关系作了较多干预，但这并不影响其合同关系的本质。

认证机构与电子签名人之间的合同是提供服务的合同，它属于无名合同。双方的权利义务在受到《合同法》及相关法律调整的同时，更多的可由双方的约定来规范。在实务操作中，由于用户更多的是对相关条款进行“接受”或“拒绝”的选择，一般很难改变认证机构业务规范，它又具有格式合同的特点。

2. 认证机构与电子签名依赖方之间的法律关系

认证机构通过签发证书提供一系列信息，包括电子签名人的名称、公钥、证书的有效期等，这些信息是进行网上交易必须的前提，是电子商务交易人所关心并且很难亲自得知的基本信息。证书信息是经过认证机构核实的真实信息，认证机构应对证书信息的真实性负法律责任。

电子签名依赖方是基于对认证证书的信赖而与交易对方进行交易的人，在实践中依赖方与认证机构之间的关系主要有 3 种情形：一是交易双方签名人与依赖方都是同一认证机构的用户，都持有电子认证证书；二是交易双方都持有电子认证证书，但是由不同认证机构发放的；三是依赖方不持有任何电子认证证书。

在第一种情形下，依赖方与认证机构之间存在认证服务合同，第二、三种情况，依赖方与认证机构之间没有合同，他完全是基于对认证机构的信任，而相信电子签名人。不论上述哪种情况，依赖方对认证机构的信赖都是始终存在的。

在电子认证活动中，电子签名依赖方与认证机构之间是一种利益信赖关系，其产生的经济根源在于电子签名人向认证机构的付费行为。电子认证证书的公正性是认证机构业务存在的根本条件，签名人正是源于电子认证证书的信用证明力，愿意向认证机构支付费用，如因认证机构与依赖方之间不存在服务合同，而偏袒建立服务合同的签名人一方，其签发的证书就会因公正性的缺失，而没有了证明力、生命力，认证机构也就没有存在的必要。因此，认证机构向依赖方提供信用服务，承担相应义务，是认证行为的内涵，签名人的付费行为是认证机构对依赖方承担义务的根源。

同时应看到认证机构对依赖方承担的义务，是有关认证法律制度规定的，是一种法定义务，不是合同约定的，须依照法律履行。在电子交易过程中，电子签名依赖方常处于弱势地位，需要法律加以重点保护。建立完善的法律救济机制能够增强电子签名依赖方网上交易的信心，促进电子商务环境的发展。

3. 电子签名人与电子签名依赖方之间的法律关系

电子签名人与电子签名依赖方通常是网上交易的双方，他们之间是一种买卖合同关系，与普通的买卖关系并无大异，只是交易形式由面对面变为网上交易。电子认证证书是交易成立的前提，电子交易依赖方基于证书信息信任对方，与之发生买卖关系。一旦因证书信息的错误造成损失，在认证机构有过错的情况下，电子签名人或依赖方均可向其追偿。

另外，在电子认证服务过程中，为了使认证机构能够维持足够的能力来履行义务和承担责任，维护其安全运营，国家主管机关依法对认证机构实施监督管理。他们之间是一种行政法律关系，在此不作赘述。

8.5.2 电子认证中心的法律责任

1. 认证机构的法律责任的归责原则

认证机构是在电子商务交易活动过程中，为交易当事人双方提供验证的第三方机构，它不仅要对参与电子商务交易的当事人双方负责，而且还要对整个电子商务交易秩序负责，因此，认证机构在与证书申请人和证书信赖人之间的法律关系当中，应负重要的法律责任。首先需要探讨的是认证机构法律责任的归责原则。

1) 认证机构的违约责任

(1) 无过错责任说。这种观点认为只要有损害发生，证书申请人就可以向认证机构要求损害赔偿，而不需要举证证明认证机构是否有过错或过失。

(2) 过错责任说。这种观点则认为一旦损害发生，证书申请人必须举证证明认证机构的确有过错，才能够请求认证机构就其损失承担责任。认证机构通常可能犯的过错是：签发错误的认证证书，未依法定规则颁发、中止或废止认证证书；认证机构的管理上的过失等。

比较以上两种归责原则，在违约责任的归责原则上倾向于应采用过错责任说的观点。因为如果采用无过错责任原则，将会使认证机构承担太大的责任风险，将导致没有从业者愿意从事认证服务的局面，从而会妨碍电子交易的进行，最终影响到电子商务事业的蓬勃发展。而采取过错责任原则比较适合我国电子商务贸易的发展现状。首先，可以激励从业者参与认证活动的积极性，推进电子认证事业的发展。其次，消费者的权益也可以得到保

护，主要是通过国家主管机关对认证机构的强有力的监督，保证认证机构依法办事、恪尽职守、努力开展好电子认证活动。

2) 认证机构的侵权责任

如前所述，采用无过错责任原则对于认证机构是非常苛刻的，因而有电子认证立法的国家都排除了无过错责任原则的适用，都确认过错责任原则为认证机构的侵权责任的归责原则。首先，由于认证服务活动是一种专业性较强的信用服务活动，证书信赖人只能了解到认证机构的对外服务功能，而对认证机构的内部操作流程和工作机制必定会缺乏了解。一旦出现错误认证的情况，证书信赖人很难证明认证机构有过错。因此，只有实行举证责任倒置，由认证机构来举证自己无过错，否则，认证机构就应承担赔偿责任。其次，由于认证机构在电子认证活动中的核心地位，有关电子认证的法律正是为推动电子认证事业的发展而制定的，认证机构十分熟悉他们自身的职责，因而认证机构对于避免自身的风险、承担责任还是早有准备的。

基于以上两点，认证机构的侵权责任应当采用过错推定原则，以减轻证书信赖人的举证困难，进而有力地维护证书信赖人的利益。

2. 认证机构对证书申请人和信赖人应承担的法律责任

1) 认证机构的违约责任与侵权责任的划分

违约责任是违反合同约定义务的法律后果，而侵权责任是违反法定义务的法律后果，两者的界限划分应在于加害方与受害方之间是否存在合同关系。在电子认证活动中，认证机构与证书申请人之间应存在服务合同关系，如果认证机构因其过错不能完成认证证书的及时发放或中止，应承担违约责任；而在认证机构与证书信赖人之间并未有合同关系存在，但是基于维护交易安全的目的，认证机构应对证书信赖人负有法定义务，如果认证机构违反了公正发布信息的义务，因此给证书信赖人造成财产损失的，应承担侵权责任。

因此，在电子认证活动中，对证书申请人的救济依靠的是对认证机构违约责任的追究，而对证书信赖人的救济依靠的则是对认证机构侵权责任的追究。

2) 认证机构对证书申请人和信赖人应承担的法律责任

认证机构对证书申请人和信赖人可能承担的法律责任，有以下几种情形。

(1) 依法承担侵权责任。各国法律几乎都明确规定，认证机构应对证书申请人和信赖人负法定的保证义务，如果认证机构违反其法定的保证义务，给证书申请人和信赖人造成损害的，证书申请人和信赖人可依法向认证机构请求损害赔偿。比如美国犹他州《数字签名法》第 46-3-303 条第(1)款规定，“经批准成立的认证机构，就其签发的证书，对证书上所载的申请人做出下列保证：①该证书无认证机构所知的虚假信息；②该证书合乎本章所规定的所有实质要件；③该认证机构于签发此证书时并未逾越其被许可的范围；④认证机构不得拒绝或限制上述保证。”

(2) 依合同所产生的违约责任。在电子交易的认证体系中，证书申请人与认证机构之间形成的是服务合同关系，因此，只要两者之间发生纠纷，并且诉讼到法院，法院便可以依据合同内容，判定认证机构是否向证书申请人负债务不履行的损害赔偿责任。

(3) 因故意泄露秘密的刑事责任。各国法律都规定，如果认证机构故意泄露证书申请人的信息资料或私钥，应承担刑事责任。比如，我国《刑法》第二百一十九条规定了侵犯

商业秘密罪，如果认证机构泄漏了证书申请人的信息资料或私钥，而且责任在于其工作人员时，可以依照《刑法》第二百一十九条的规定，上述行为若对证书申请人造成重大损失的：“处三年以上七年以下有期徒刑， 并处罚金……”。如果责任在于认证机构本身，可以依照《刑法》第二百二十条规定：“单位犯本节第二百一十三条至第二百一十九条规定之罪的，对单位判处罚金，并对其直接负责的主管人员和其他责任人员，依照本节各该条的规定处罚”。

8.5.3 我国第三方认证相关立法

1. 电子签名法

1999 年，我国修改后的《合同法》承认了数据电文，包括传真、电子邮件的法律效力。但是一旦发生纠纷，法院仍无法将这些传真、电子邮件作为证据，数据电文形式的合同双方仍承担着巨大的法律风险。为规范电子商务行为、给电子商务发展提供必要的法律保障，2005 年的 8 月 28 日，全国人大常委会审议通过了《电子签名法》草案，并定于 2005 年 4 月 1 日起实施。至此，以法律的形式首次赋予可靠的电子签名与手写签名或盖章具有同等的法律效力，并明确了电子认证服务的市场准入制度。《电子签名法》的出台是我国电子商务发展中的一座里程碑，它对保证电子商务交易、促进电子商务发展具有举足轻重的意义，而且对今后电子政务以及未来全民的社会信息化都将产生深远的影响。

在我国的《电子签名法》中，尽管主要内容是对电子签名的法律地位给予确认，但该法还是对电子认证机构的市场准入、监管作了一些原则性的规定，并且首次以法律的形式对电子认证机构的一些法律责任问题做出了规定。如对电子认证机构承担过错责任的问题作出明确规定，只要电子认证机构提供的电子签名认证服务中存在过错，就要赔偿证书用户和证书依赖人所遭受的损失，并且有无过错的举证责任也由电子认证机构承担。就电子认证机构电子签名领域的安全保障机构在整个电子商务中的特殊地位而言，科学合理地界定其所应当承担的民事责任，无疑是保证第三方机构乃至整个电子商务稳健发展的前提，但由于该法立法宗旨定位于确认电子签名的法律效力，因而对电子认证机构的民事责任问题规范的较为笼统，特别是对电子认证机构违约或侵权造成的赔偿问题，没有作任何明确的规定，只是从行政处罚的角度，谈到了对电子认证机构的处罚问题。

2. 电子认证服务管理办法

为了配套《电子签名法》的实施，进一步规范电子认证服务行为，对电子认证服务提供者实施监督管理，同《电子签名法》一起生效的还有一部由信息产业部颁布的《电子认证服务管理办法》(以下简称《管理办法》)。该办法以电子认证服务机构为主线，围绕电子认证机构的设立、电子认证服务、数字证书的内容、撤销证书的几种情况以及电子认证机构的审查、监督管理和处罚等几个方面的内容做出了明确规定。在内容上，《管理办法》比《电子签名法》更为详细的规范了电子认证机构的行为，其目的主要是解决电子认证服务行政许可的实施和电子认证服务机构的监督管理问题，保证电子签名法的顺利施行。

从表面上看，以信息产业部第 35 号部令形式出现的《管理办法》只是一部部门规章，但因为它是国家法律特别授权制定与《电子签名法》配套同步实施的，因此有别于一般的部门规章而具有重要法律效力和作用。通观法条，笔者注意到，一方面《管理办法》受自

身地位所限，无法就电子认证机构民事责任问题作更多规范；另一方面，虽然按照《电子签名法》的要求设定了电子认证业务规则的备案制度，但却缺乏电子认证的行政主管部门对备案材料应当履行实质性审查的相应规定。在实践中，已有许多电子认证机构利用这一缺陷，任意扩大自身的权利而缩小与之相对应的义务，这导致了电子认证业务规则备案制度流于形式，难以发挥其应有的作用。

3. 地方相关电子认证立法

我国的电子认证立法一个明显的特点就是地方先于国家。早在 1999 年的“两会”期间，就有人大提案提出了电子商务立法的问题，鉴于当时条件的不成熟，该提案并没有得以立即实现，而当时国内已经有了 70 多家的电子认证服务机构，已发出去上百万张数字证书，这些电子认证机构有行业的、区域的，也有完全市场化的；这些数字证书有发给企业的、个人的，也有发给服务器的。一些在电子认证领域已经积累了一定实际经验的省、市则开始探索出台相关地方性法规，规范本地电子认证机构的行为。这其中主要有：海南省于 2001 年 4 月 1 日通过了《海南省数字证书管理试行办法》，2001 年 10 月 31 日海南省信息产业局颁布了《海南省数字证书认证机构资格认定办法》，上海市于 2003 年 1 月 1 日起开始实行的《上海市数字认证管理办法》以及广东省于 2003 年 2 月 1 日出台的《广东省电子交易条例》等。其中，《广东省电子交易条例》是全国首部有关电子商务管理方面的法规。该法规对确立电子签名的法律地位、规范电子认证机构的管理、规范电子交易服务提供商的管理作了规定。

这些地方性法律法规的出台在当时有一定的积极意义，一方面使当地的电子认证机构的管理和运营有法可依，又为全国立法提供了借鉴和参考；但另一方面，由于各地地方观念的局限性，致使各地具体的规定不尽相同，造成了各地电子认证机构的设立条件、技术标准等方面的不统一，也为电子认证机构以后的发展制造了人为的障碍，对进一步规范电子认证市场带来了一定负面影响。

8.5.4 认证中心的设立、终止及监管

1. 认证机构的设立

鉴于认证机构的核心地位，它的设立是电子认证制度中重要的一环，各国法律大都对此进行了相应规定。

1) 设立的方式

对认证机构的设立各国依据其不同国情采取了不同的方式，总体来看主要有特许制、批准制及备案制。

(1) 特许制也称强制许可制度，属政府主导型，是最严格的设立方式。由政府相关的审批机构制定要件，并在申请者提出申请后，进行严格审查，决定是否核准其成立。多数发展中国家，由于市场发展不完善，加之技术资金等方面的限制，采取政府干预方式，以促进和保障本国电子认证体系的建立。韩国、日本在认证机构的设立上也采用了此种方式。

(2) 批准制，属政府引导型，是一种弱限制方式。审批机构可依据国家政策和当前需要制定一系列要件，提出申请者如符合要件要求，便可批准其成立。采用这种方式管理认证机构的国家大多规定了自愿认可制度，认证机构并不一定要取得许可，但经政府许可的

认证机构可享受责任限额等优惠条件。政府对认证机构管理只实行有限介入，不进行全面干预。例如，新加坡《电子交易法》规定，只要认证机构的电子证书载明标准并符合一般认证原则，均可承认。但安全认证机构可以自愿向管理机构申请许可，虽然管理机构的许可并不妨碍安全认证机构进入市场，但是得到许可的安全认证机构可以享受某种“优惠”，尤其是可以享受法律规定的责任限制。

(3) 备案制，属主管机关权限最弱的方式。从业者只需向审批机构履行备案手续即可。该方式奉行政府不介入，不干预，让认证机构通过行业自律，在市场竞争中建立信用。这是市场自由、技术中立原则的充分体现。采用这种模式的国家主要是欧盟各国，欧盟《电子签名指令》第三条规定：“成员国不得为证书服务规定任何事先授权。成员国可以为提高证书服务引进或维持一套自愿认可的方案……”。

我国《电子签名法》第十八条规定：“从事电子认证服务，应向国务院信息产业主管部门提出申请，并提交符合本法第十七条规定条件的相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，自接到申请之日起四十五日内做出许可或不予许可的决定。予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。”

可见我国现阶段认证机构的设立方式采取的是政府主导的强制许可制。有人认为对认证机构的设立应采取发达国家的经验，依靠市场力量进行调节，通过行业自律予以规范，政府不介入其中，对其加以过多限制，以免阻碍认证市场的发展。但同时必须看到，当前我国市场经济体系不够完善，第三方认证体系尚未完全建立，社会信用制度不健全，电子商务与信息化发展不均衡，其安全性还有待提高，在这种大环境下，为保障电子商务的健康发展，采取行政特许模式是与我国目前基本国情相适应的，有利于电子认证行业的市场培育和发展。

2) 认证机构设立的条件

认证机构从事电子认证服务应具备实质要件和形式要件两方面的条件，下面以实质要件为主加以讨论。

(1) 实质要件。认证机构申请从事电子认证服务时，需要满足一定的审批条件，政府主管部门需要从主体资格、从业人员、设备、场所、资金等方面进行审查。

① 主体资格。认证机构需要具有从事信用服务的素质和资格，又要承担因认证业务而产生的财产责任，因此对其发起人应有一定要求。各国和地区根据自身情况进行相关规定，大部分国家的法律只允许法人机构作为认证机构的发起人；而有些国家和地区的法律则规定，无论法人或个人，均可成为认证机构的发起人。如美国犹他州规定，自然人与法人，均可成为认证机构的发起人，不过作为发起人的自然人，仅限于从事律师及公证业务的专业人员，并非无任何限制。

从我国目前情况看，自然人不适宜作为认证机构的发起人，因为自然人承担财产责任的能力，一般不如法人机构，另外，自然人的生老病死，都会影响到业务的稳定。虽然《电子签名法》中对此项未做明确规定，但《电子认证服务管理办法》第五条规定“电子认证服务机构应当具有独立的企业法人资格”，可见我国目前设立的认证机构都是独立的法人机构，不允许自然人作为认证机构的发起人。

② 从业人员。认证机构所从事的业务是一项具有高技术含量的工作，要求从业的技术

人员应当具备认证工作所必需的技术水平和素质。同时，由于认证工作涉及审查客户资料，并签发证书，关系贸易活动的安全，要求从业人员具有良好的品质。对从业人员的要求是认证机构安全运作的必要条件，法律一般对从业人员规定严格的技术条件和素质条件，有些国家还设立了从业禁止条件，防止因内部从业人员的行为危害电子商务活动的安全。例如美国犹他州电子签名法中规定从业人员不得有重大犯罪的前科或犯有其他欺诈、虚伪陈述或欺骗等罪行。我国《电子签名法》第十七条中规定，“提供电子认证服务，应具有与提供电子认证服务相适应的专业技术人员和管理人员”。

③ 设备要求。认证机构所需设备包括硬件和软件两个方面。认证工作对专业技术的要求很高，为了满足需要，认证机构所使用的设备必须是质量合格并合法使用。信息产业发展迅速，技术与产品都在不断更新升级，因此不宜以法律形式对其做具体规定，其标准应由主管部门根据技术发展现状做出要求。认证系统的软件须经相应的政府安全机构检验。我国《电子签名法》第十七条中规定，“提供电子认证服务，应具有符合国家安全标准的技术与设备，应具有国家密码管理机构同意使用密码的证明文件”。

④ 场所和资金。认证机构的营业场所，通常与其业务进行地是一致的。认证机构是一种在线信息服务，其场所可不在业务开展地，但政府部门为了便于对其行使管辖权，一般会要求营业场所固定存在。我国目前所设立的认证机构，都存在固定的营业场所。认证机构可能会由于认证活动的失误等给当事人造成损失，而这种损失的数额可能是相当大，这就需要认证机构有一定规模的资金，能够承担相应的责任。我国《电子签名法》第十七条中规定，“提供电子认证服务，应具有与提供电子认证相适应的资金和营业场所”。在资金方面，《电子认证服务管理办法》更明确规定：“注册资金不低于人民币三千万元。”

(2) 形式要件。形式要件是提供认证服务之前必须履行的有关程序，我国《电子签名法》规定，“申请人向国务院信息产业主管部门提交申请，提交符合第十七条规定的有关文件，信息产业部依法审查并做出许可后，向申请人颁发电子认证许可证书；申请人持许可证向工商行政管理部门办理企业登记手续；最后，获得认证资格的机构在互联网公布其名称、许可证号等信息”。

2. 认证机构的终止

认证机构是一个营业性实体，它所从事的信用服务，是一般交易的基础条件，涉及商业交易的通畅与安全。认证机构一旦终止其业务，它过去签发的证书的有效性就无法再由其给予证明，这将会给证书持有者和证书依赖方带来不便或损害。因此，认证机构的不间断运作与社会公众的利益密切相关，其业务终止，不像一般赢利性企业一样，在清算之后完全结束，而应做出必要的预先安排和相应程序，建立使其营业持续进行的机制。一般应包括：①事前通知，在认证机构终止之前，必须通知用户和潜在依赖方，同时报告主管机关；②安排业务承接，为了提供不间断的认证机构服务，终止的认证机构可与其他认证机构就业务承接进行协商，妥善安排。

对认证机构的终止做出相关规定，可以为认证机构客户的利益提供确实保障，是十分必要的。许多国家对此都进行了严格的规定。日本《电子签章与认证服务法》第十条规定：“认证机构终止其经许可之认证服务时，应依主管机关之行政命令，事先向主管机关申报，而主管机关应将该认证机构申报之事实公告周知。”德国《信息与通信服务法》第十一条

规定:“①证机构一旦停止业务，即应在尽早时间内通知主管机关，并确保在停止业务时有效的证书由另一认证机构接手或被撤销；②应将有关文件移交给接收的认证机构或提交给主管机关；③如申请破产或争端，应毫不迟延地通知主管机构。”

我国《电子签名法》第二十三条对该问题也进行了规定，“电子认证服务提供者拟暂停或终止电子认证服务的，应当在暂停或终止服务九十日前，就业务承接及其他有关事项通知有关各方；应当在暂停或终止服务六十日前向国务院信息产业主管部门报告，并与其他电子认证服务提供者就业务承接进行协商，做出妥善安排。认证服务提供者未能就业务承接事项与其他电子认证服务提供者达成协议的，应当申请国务院信息产业主管部门安排其他电子认证服务提供者承接其业务。”

3. 认证机构的监管

认证机构提供的信息服务不同于单纯的商事交易，它在电子交易中起着重要作用，为了维护认证机构的安全运营，应对其进行必要的监管。一般来说，各个国家都由某部门统一负责认证机构的监管，目的在于确保认证机构能够维持足够的能力来履行其义务和承担责任。这种监督主要体现在制定规范和业务监管两个方面。

1) 制定规范

认证机构的业务开展有赖于采用的技术和服务标准，如果各认证机构各自为政，自我发展，在技术上没有统一的标准，很难实现其兼容性，从而使电子认证变得无法实施。政府主管部门可规定统一的技术方案，并规范不同级别的认证机构的电子认证标准及程序。

我国信息产业部电子认证服务管理办公室，为了规范电子认证业务规则的基本框架、主要内容和编写格式,根据当前电子认证系统大多采用基于非对称密钥的 PKI 技术的现状，参考国家标准化部门的相关标准，于 2005 年 4 月编制了《电子认证业务规则规范(试行)》。要求电子认证服务机构应参照该规范，结合电子认证业务的具体情况，编制电子认证业务规则。

2) 业务监管

监管机构应定期对认证机构进行检查，并被允许在营业时间进入认证机构的工作地点进行现场核查；应及时统计认证机构的相关信息；对认证机构不遵守认证业务准则或有其他违法行为的，监管机构有权按照法律法规的规定对认证机构予以行政处罚，直至吊销其从事认证活动的营业执照。

我国《电子签名法》规定：“国务院信息产业主管部门依照本法制定电子认证服务业的具体管理办法，对电子认证提供者依法实施监督管理。”

本 章 小 结

网络支付是在信息技术发展到一定程度下应运而生的，与传统的支付手段在本质上并无二致，然而由于它完全依赖于网络和信息技术的特点，这就使得对它的监管与传统支付有着巨大的区别。

网络支付的过程主要涉及电子货币、网络银行以及第三方支付平台等方面。电子货币是完全依赖于电子化的高新技术，它是一组虚拟的模拟数据，并以互联网技术为操作平台，正是由于这些特点使其衍生出很多不同于传统的法规与监管新问题，解决它们除了要面对传统的困难之外，还要面对技术上的难题。网络银行是具备发行、流通电子货币的机构，是网络支付中重要的一环，也是网络支付监管的重要对象。第三方支付平台是与银行达成一定协议，第三方独立机构提供的交易支持平台，电子货币的流动就发生在这个平台里，所以要维持良好的网络支付环境，对于第三方支付平台的监管是至关重要的，然而第三方支付的运营商不同于实体银行，在信誉和保障上不及银行，相关法律法规难以制定，目前仍处于逐步探索的阶段。

网络支付的法规与监管是刻不容缓的，因为网络交易的数量正在突飞猛进，第三方支付平台上流通的货币量越来越大，如何保障这些货币的安全，使得网络支付能够健康的发展需要对网络支付进行更深的探讨，以此为基础建立起规范的法律环境。

关键术语

网络支付　电子货币　网络银行　第三方支付平台　第三方认证中心　法律法规　监管

综 合 练 习

一、填空题

1．电子货币的发行同传统的货币发行大体上是相同的，却又不同于传统货币，它的_____以及对_____，又迥异于传统货币。

2．网络银行在开展各项业务时，必须通过_____、_____、_____加以规范。

3．欧盟对网络银行监管所采取的办法较新，其监管目标主要有两点：第一，_____；第二，_____。

二、判断题

1．资金划拨所涉及的当事人很多，除了顾客本人、网上银行等发行主体外，还包括资金划拨系统经营主体、通信线路提供者、计算机制造商或软件开发商等众多的相关方。（　　）

2．电子签名人与电子签名依赖方通常是网上交易的双方，交易形式由面对面变为网上交易，他们之间偏离了买卖合同关系，与普通的买卖关系差异甚大。（　　）

3．在违约责任的归责原则上倾向于应采用无过错责任说的观点。（　　）

4．信息产业发展迅速，技术与产品都在不断更新升级，应该以法律形式对其做具体规定，其标准应由主管部门根据技术发展现状做出要求。（　　）

三、选择题

1．根据《电子支付指引》规定，银行通过互联网为个人客户办理电子支付业务，除采

用数字证书、电子签名等安全认证方式外，单笔金额不应超过(　　)元人民币，每日累计金额不应超过(　　)元人民币。

A．800，4000　　B．1000，4000

C．800，5000　　D．1000，5000

2．由于网络银行的服务协议内容隐含了对高效率时间利用和使用便捷的承诺，客户通过网络银行进行支付交易时，责任一方对损害的赔偿不仅应包括对市场交易直接成本的赔偿，还应包括对(　　)的合理赔偿。

A．机会成本　　B．交易成本

C．交易效率成本　　D．隐性成本

3．下列关于电子货币与传统货币的比较，哪种说法是错误的？(　　)

A．电子货币完全虚拟化、数据化，一般不需要介质

B．从货币的流通上看，电子货币不能直接由交易双方来进行操作

C．电子货币的发行需要银行或金融信用机构，以及第三方的银行和认证体系的配合

D．大额资金在银行间转账属于传统货币资金交易的范畴

四、简答题

1．电子货币具备哪些法律属性？

2．电子货币会产生哪些常见法律问题？

3．电子货币给金融监管带来哪些新问题？

4．为加强电子货币监管，可以采取哪些措施？

5．阐述网络支付法律关系调整的基本原则。

6．网络银行中存在哪些法律风险？

7．网络银行法律监管存在哪些问题？

8．第三方支付有哪些潜在问题和风险？

9．简述我国第三方支付监管现状及监管趋势。

实际操作训练

课题：网络支付法规和监管，第三方支付平台

实训项目：辩论赛：淘宝“诚信自查活动”是否必要

实训目的：运用本章学习的法律知识，组织论据，通过辩论赛加深对本章知识的理解

实训内容：淘宝在其官方网站宣布其“诚信自查系统”上线，从而开始为期两周的诚信自查活动。学生通过网上调查，收集资料，进行一场关于网络支付主题的辩论赛

实训要求：要求收集的资料符合本章主题，论据要建立在本章的法律知识基础之上

案 例 分 析

根据分析案例所提供的资料，试分析以下问题。

1．我国对第三方网络支付业务监管的监管原则。

2．提出五个我国第三方支付发展面临的问题。

3．就相关发展问题提出新的策略和解决方案。

分析案例

专家称支付宝套现属违法行为

支付宝融资模式操作上可行

“利用支付宝实行信用卡套现，具有很强的实际可操作性。”知名电子支付研究专家，中国电子商务协会政策法律委员会张雨林表示。

具体来说，持卡人可利用亲戚或朋友的身份证和银行卡在网上开店，然后使用自己的信用卡去该店进行虚假购物。而淘宝网也无从查证该笔交易是否真实，全凭买家和卖家在网上的收货确认进行付款。

“用这种方法完全可以实现信用卡的套现，并且不花费任何费用。加之网络店铺开设的简单与快速，且不需要支付任何手续费或交纳税金，故该种套现行为的实施成本较低，其风险也只是面临支付宝公司冻结账户资金而已。”张雨林告诉记者。

从操作的结果来看，成功套现的小王按照银行信用卡的规定，在到期日之前偿还了其套现的资金。“偿还套现资金后，我并没有给银行带来不利的影响，仅仅是少支付了期间的利息而已。”小王如此表示。

而就是这种做法，在银行眼里则完全不同。“如果别人都利用支付宝来套现，而不支付期间利息，那么对银行来说，相当于放出去了一笔无息银行贷款，而且这笔无息贷款还没有任何使用范围的限制。这样的贷款能是安全的吗？”上述银行人士对利用支付宝套现的行为提出如此强烈质疑。

正因为支付宝套现具有理论可行性，少数人士也就开始利用支付宝进行融资。据了解，11 月份，淘宝网打击了多个信用卡套现团伙，涉及金额总计 100 万元。

支付宝套现违规还是违法？

对于支持支付宝套现的人士来说，他们只是利用了制度的漏洞，不属于违反国家法律，而只是违反网上交易商和银行的规定。而这也是让反对者尴尬的问题。因为如果只是违规，那么解决的办法只能是自律，但如果是违法，那么就可以动用国家的力量来解决。

那么支付宝套现到底是违规还是违法呢？一个明确的回答：违法。

“早在 1996 年 4 月 1 日，中国人民银行就颁布并实施了《信用卡业务管理办法》，其中明确规定，持卡人不允许利用信用卡套取现金以及恶意透支；1999 年 3 月 1 日，《银行卡业务管理办法》规定，利用银行卡及其机具欺诈银行资金的，根据《中华人民共和国刑法》及相关法规进行处理；2006 年 2 月底，中国人民银行和银监会发出《关于预防信用卡风险有关问题的通知》，明确规定持卡人套现和商户提供套现服务属违法行为。从目前央行制定《银行卡管理条例》的情况来看，信用卡套现行为将会进一步受到监管。”

目前存在着几种比较普遍的信用卡套现手段如下。

(1) 付手续费套现。利用商家或空头公司进行虚假交易，通过银联 POS 将信用卡上的金额划走，并且当场套现。

(2) 利用电子商务网站套现。网上交易领域，持卡人甚至可以不需要他人的帮助，只通过自买自卖的方式，就能实现信用卡套现。

(3) 刷卡购买手机充值卡。在营业厅刷卡购买话费充值卡，充进电话号码以后，销号退款。

支付宝属于第二种情况。而对于准备利用支付宝套现进行融资的人士，相关专家表示支付宝套现与融资完全是两个本质不同的问题。支付宝套现的性质就是利用支付宝实施的信用卡套现。而我国相关法规对信用卡套现行为一直持否定态度，也就是说，支付宝套现行为是违法的，违法的行为是不可能成为融资手段的。

资料来源：http://tech.sina.com.cn/i/2006-12-23/11031303283.shtml.