第三方支付企业功能分化风险控制成重要标志电子商务考试
 第三方支付平台已经不再是被轻视的力量，随着网上交易日益增多，支付平台的交易额也在迅速增加，电子支付的资金流量随之迅速增长，带来了支付厂商们对支付风险的重新评估。 一些厂商正在考虑更换更大容量的服务器，另一些厂商则思考着如何更新系统，以完成每秒数次的交易流量。而在快速膨胀的交易流量中，如何防范包括洗钱、恶意支付、外卡诈骗等新出现的风险，又成为了摆在第三方支付厂商面前的重要课题。 数年前，有客户持国外信用卡，通过国内的某第三方支付平台在国内的一家零售网站上购买了数万元的产品，事后拒付相关款项，但商品却已经送到对方手中。此案几乎成为了一桩悬案：通常银行在与第三方服务机构签定合作协议时，都会把自己的责任撇清，而第三方支付厂商其实只提供了一个从商家到银行的管道而已，似乎也不应该承担责任。“ 嫌疑犯是从这条高速公路跑掉的，但怎么能定公路的罪呢？ ”一位业内人士如是说。那么商家的损失究竟应该由谁来承担？ 保障交易安全已经在一些支付厂商处得到重视，但当第三方支付厂商在研究风险控制时，却又处在极其不利的地位。自身资源的欠缺，使其只能缓慢地发展。但换一个角度，当第三方支付厂商的风险控制能力提升，有了成熟的产品时，则将可能成为第三方支付厂商出现分化的一个标志。 难以获得合作伙伴支持 Paypal，作为业内最大的第三方支付厂商，其年交易额已经超过了400亿美元，该数字大约是国内网络支付总额

的9倍。Paypal是不多的同Visa等发卡组织形成了密切合作的第三方支付厂商。当有在Visa数据库中显示有恶意交易倾向的信用卡通过Paypal交易时，Paypal就会得到相关数据提醒，从而尽早防范，避免进一步的损失。“国内的第三方支付厂商中没有人能获得这样的支持。”一位知情者告诉记者。所以，在国内防范外卡诈骗就成了一道难题。“在Visa这样的发卡组织看来，国内的第三方支付厂商只是他们的商户，而不是他们的会员，所以无法获得他们的资料。”在另一方面，国内银行所掌握的风险控制数据，在各合作银行间实现共享都形成了困难，就更难以使第三方支付厂商们获益。“比如支付厂商侦测到有恶意交易嫌疑的交易，如果想通过更多的交易信息，比如银行卡户主信息等内容判断该交易是否恶意，就需要另行查证，而无法直接通过数据共享的方式找到答案。”一位知情人士说。随着2008年北京奥运会的临近，外卡支付渐渐成为令人关注的热点。在北京商家大面积普及推广刷卡系统的同时，外卡的网上支付也将迎来突破性的增长。而外卡诈骗历来是国内第三方支付厂商风险防范的难点。“我们是国内最早实现外卡支付的第三方支付厂商。”环讯支付相关人员对记者说，在外卡支付的管理经验方面，环讯也有着自己丰富的经验。“我们有相应的系统对外卡支付风险进行防范，比如说，信用卡卡号的前6位代表了发卡行，一些诈骗者会利用前6位数字相同的信用卡集中进行交易，我们对这种方式能够很好地监控。另外，在同一张信用卡的频繁交易方面，也可以实现监控。”防范盗卡支付“国内的银行卡大都有密码，风险相对外卡要小很多。”一位业内人士说，但是，在国内银行业纷纷上网的环境下，银行卡的风险

也在发生着变化。一位民生银行的用户王先生从来没有用银行卡进行过网上交易，也没有丢失过银行卡，但他的银行卡账户上的14000余元却被人通过一家第三方支付平台，在连续三天集中进行了恶意消费。 目前，越来越多的银行已经不再默认银行卡可直接上网，而是用户通过申请并认证的方式，才可开通网上银行，但多数情况下，用户只需要使用自己的银行卡卡号和密码，在网上提交一个申请，即可开通网上银行。国内某高校的网站上曾经存放了一份包含新入学学生办理银行卡卡号的文件，该文件被一名普通的网民在无意中用搜索引擎搜到后，猜中了大部分银行卡的密码，然后通过网上银行，把这些银行卡内的资金盗取一空。百考试题收集整理 如何防范盗卡者在网上恶意支付，就连银行业自身也没有强有力的手段来避免，而对于第三方支付厂商来说，在缺少必要信息支持的环境下，建立这样的风险控制系统就更为艰难。“ 即时防范几乎是不可能的事，只有在事后，银行方面向我们提供了被盗银行卡的用户信息，我们才能发现该银行卡被盗刷了，而这时候资金都已经交割完毕，追回的难度很大。 ”一家支付厂商说。 在风险控制方面，快钱公司建立了专门的风险控制部门和专门的风险控制机制。 在建立相应的风险控制机制防范的基础上，快钱得到了很多有关恶意支付的防范案例。比如，2005年10月17日，快钱风险控制部在处理客户结算申请时发现一笔可疑交易，由客户肖某提交，金额共计1000元，款项来源是农业银行卡充值，结算的目标账户是一张交通银行的借记卡，该借记卡的发卡地为广东深圳。风险部随即向农业银行发出查询申请，次日得到回复，这1000元资金来源于北京农行卡，户名为李某，而非肖某。

风险部人员通过肖某的资料与其联系，但始终得不到肖某的回复，接着风险部人员通过农业银行提供的信息与李某取得联系，方得知该银行卡已经有1年左右没有使用过，是李某以前工作单位帮她办理的工资卡，她从未更改过该银行卡的密码，也从来不网上支付。风险部分析后认为，李某的账户卡号有很多种途径可以被犯罪分子取得，而且其密码过于简单，很容易被人猜中，然后被人在网上进行恶意支付。因为发现得及时，该交易被止付，资金被追回。 防范恶意支付的重要资源来源于数据。如果交易厂商自身流量较小，历史数据比较少，在得不到银行数据支持的情况下，就难以对新产生的资金流量进行有效的监控。易宝支付一直以来在做风险控制系统，并且与一些银行达成了部分数据共享的合作。易宝支付副总裁余晨告诉记者，易宝支付在技术手段加密的基础上，以商业逻辑判断恶意支付行为。“ 比如外卡，如果它用来支付酒店的费用，这比较正常，而如果它是去国美买一台电视机（不可能把电视机搬到国外去），就可能有风险了，对于类似这样的行为，可以进行一定的监控。 ”百考试题编辑整理 而在风险控制方面，因为不同银行的相关政策不同，共享给第三方支付厂商的数据也不相同，但较敏感的数据，如银行卡账户信息等，各银行都实行保密政策。在这种情况下，第三方支付厂商除了能够与部分提供了黑名单数据的银行共享一些历史交易纪录之外，更多情况下，是通过正常的商业逻辑来发现恶意交易行为。“ 比如说一张卡集中大额度消费、同一IP多张卡集中消费等，我们的监控系统都能够发现。 ”余晨说。 随着第三方支付厂商自身体系建设越来越成熟，在风险控制方面，各厂商也都在采取不同的手段，建立

自己的风险控制机制。而成熟的风险控制体系将为客户带来最好的用户体验。从IT企业向真正的金融机构过渡，风险控制将成为必然的热门。对于第三方支付企业来说，风险控制体系方面的差异，也将成为他们之间发生分化的重要标志。F8F8" 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com