企业数据管理解决方案
执行简报
2008 年 3 月

IBM Information Management software

支付卡行业数据安全标准（PCI DSS）：解决内部威胁

目录

为何关注支付卡和隐私遵从性？

用作商品和服务交换中的一种货币形式，支付卡无疑是支撑全球经济增长的主要部分。例如，单在美国，每年循环帐户中就有大约 6.41 亿张信用卡，其消费性开支约 1.5 万亿美元。[1] 同样，在 2007 年 10 月和 12 月之间，英国消费者使用信用卡消费 324 亿英镑，为有史以来的第二大数额。同期，使用借记卡的消费达 590 亿英镑，为 2000 年首次记录借记支出以来的最高值。[2]

但是，令人瞩目的数据泄露问题的日益增加已经暴露出没有妥善保护机密客户信息的支付卡处理器、销售点情报系统供应商和金融机构的脆弱性。据 Privacy Rights Clearing House 报导，在美国从 2005 年 1 月到 2008 年 3 月有超过 2.18 亿条个人可识别记录被公开，造成损失达数十亿美元。[3]

面对客户信息的盗用和滥用所引起的日益增长的风险和资金损失，支付卡行业不得不主动出击。PCI DSS 即为支付卡行业对这些侵害问题的响应。在未来，不能保护消费者支付卡信息的贸易商和零售商将承担责任。

关于 PCI DSS

PCI DSS 是一个涉及多方面内容的法规集合，定义了对实施安全管理策略、程序、网络架构、软件设计以及其他重要保护措施的要求。其目的在于提高电子付

款的安全性，PCI DSS 代表一个保护所存储、传输或处理的持卡人数据信息的统一行业标准。

PCI DSS 是由万事达（MasterCard Worldwide）和 Visa 国际组织于 2005 年 1 月发起的，后由美国运通（*AMERICAN EXPRESS*）认可。为了响应大量的数据涌现和侵犯隐私的身份盗窃、以及盗用持卡人数据信息而进行的欺诈，该标准不断得到发展。

2006 年 9 月，Visa 国际组织、万事达（MasterCard Worldwide）、JCB International、Discover Financial Services 和美国运通组成了一个独立的机构，支付卡行业数据安全委员会，以监督该标准的实施。该委员会的任务是通过扶持 PCI DSS 的广泛采用来提升支付帐户数据安全。

PCI DSS 的要求有哪些？PCI DSS 的主要目标是确保持卡人数据信息得到保护。该标准包括 5 大类 12 项要求，重点强调数据验证、访问控制、审计和数据加密。

为遵从此标准，处理支付卡信息的公司被要求建立严格的安全策略、流程和程序。[4]

该标准涵盖了维护安全网络、保护持卡人信息、管理风险、实施控制措施和监控测试网络等大量问题（参见表 1）。

表 1. PCI DSS 的要求*

构建和维护一个安全网络	
1	安装并维护一个防火墙配置以保护持卡人数据信息
2	不使用供应商提供的口令以及其他安全参数方面的缺省配置保护
持卡人数据信息	
3	保护所存储的持卡人数据信息
4	在公众、开放的网络上传输持卡人数据时，需要加密
	维护一个脆弱性管理程序
5	使用并定期更新反病毒软件
6	开发并维护安全的系统和应用
实施功能强大的访问控制措施	
7	按照“按需知道”的原则严格限制对持卡人数据信息的访问
8	向访问计算机的每个人都分配一个唯一的帐号 ID
9	严格限制对持卡人数据信息的物理访问
定期监视和测试网络	
10	跟踪并监视对网络资源和持卡人数据信息的所有访问
11	定期测试安全系统和流程
维护一套信息安全策略	
12	维护旨在解决信息安全问题的策略

*支付卡行业(PCI)数据安全标准 —— 版本 1.1。支付卡行业安全标准委员会，2006 年 9 月。

带格式的：项目符号和编号

谁必须遵守 PCI DSS？为保护机密的持卡人数据信息，无论实体的规模和所处理的交易量多大，存储、处理或传输持卡人信息的所有成员、贸易商和服务提供商都必须实施该标准。**而且 PCI DSS 的要求不仅仅适用于电子数据。**各种企业有义务以适当的方式处理包含支付卡细节和信用卡持卡人数据信息的印刷资料。

根据每年所处理的交易量，可将发生支付卡交易的所有贸易商分为以下级别。

- 第 1 级：拥有 600 万次卡交易的贸易商和已经危及持卡人数据信息安全的贸易商
- 第 2 级：卡交易在 100 万次到 600 万次之间的贸易商
- 第 3 级：卡交易 20,000 次到 100 万次之间的贸易商
- 第 4 级：所有其他贸易商

这些级别决定了贸易商必须进行的验证流程，从而获得并保持遵从性。
处理信用卡交易的所有服务提供商分为以下级别：

- 第 1 级：所有支付处理器和支付网关
- 第 2 级：不属于第 1 级但拥有超过 100 万信用卡帐户或交易的所有服务提供商。

- 第 3 级：不属于第 1 级而每年信用卡帐户或交易数低于 100 万的服务提供商。

这些级别决定了服务提供商必须进行的验证流程，以获得并保持遵从性。

为什么要采取措施来遵守这些规定？

如果不进行适当的控制来保护持卡人数据信息，您的机构会有更大风险成为数据泄露的受害者。其后果包括且不限于市场份额损失、品牌损害、客户忠诚度和收入损失。

Ponemon Institute 对小额银行业务客户的一项研究提出，消费者只与能保护其隐私的零售商做生意。该研究表明，一个公司仅仅泄露隐私一次，就会有 34% 的客户停止与其的贸易。当个人信息被泄露两次后，该数字将增加至 45%。根据这项研究，“信任感可转变为高度的品牌忠诚，而对银行数据安全功能的信心丧失可能导致大量客户流失。”[5] 这种流失的一个重要原因是 2006 年美国消费者确认被盗的金钱大约有 493 亿美元。这些消费者仅为了执行善后措施并恢复信用记录平均每人就要花费 535 美元。[6]

避免因不遵从法规而受高额罚款。不符合 PCI DSS 标准的大代价包括针对每次事件可能高达 500,000 美元的罚款。例如，2006 年间 Visa 对 77 家公司的罚款总额为 470 万美元，2005 年的 32 次罚款总计金额为 340 万美元。

而且，最严重的惩罚可以使一家贸易商破产。支付卡公司可以限制甚至撤销贸易商接受支付卡付款的能力。

人们往往忽略与数据泄露后做出的适当响应相关的费用。数据泄漏后会有更多的员工来回应客户的咨询和关注、处理公共关系，以修复在媒体中受损的声誉。这些相关费用包括由此而支付的费用，以及由于不妥善保护数据而招致的诉讼开支。

该标准的基本要求是保护消费者信息不受欺诈，不得随意滥用。如果您的组织要管理、存储、传输或处理持卡人数据信息，您必须适当防范以保护这种机密信息。企业是建立在消费者信任和忠诚基础上的，任何破坏信任的行为将带来灾难性的金融后果。

采取措施以减少数据泄露的风险。几大零售商已经不幸成为大量数据泄露的受害者。T.J. Maxx[7]、BJ's Wholesale Club、DSW 和 Polo Ralph Lauren 都曾经历过数据泄露，这将其大量客户的私人数据信息置于危险境地。

T.J. Maxx 事件首次被发现是在 2006 年 12 月，该公司处理和存储客户交易（包括信用卡、借记卡、个人支票和退货交易）信息的计算机系统遭遇了“未经验证的入侵”。黑客本可以偷走美国、加拿大和波多黎各的交易信息。

最终，这次入侵可能影响美国、英国、爱尔兰和其他国家的众多信用卡公司和成千上万的消费者。[8]

据联邦贸易委员会称，BJ's Wholesale Club 松懈的数据安全措施导致在非 BJ's 商店发生了一系列欺骗性购物。这些购物使用伪造的信用卡进行， 这些信用卡含有 BJ's 以前从客户信用卡磁条中收集的个人信息。因此，受到欺诈损害的金融机构起诉 BJ's，要求赔偿损失。按照解决条款，BJ 's 将执行综合信息安全项目，并在未来 20 年内每年都接受第三方审计。

在 DSW 的案例中，据其母公司 Retail Ventures 所言，大约 140 万张信用卡和 96,000 条支票交易信息从 108 家 DSW 鞋店被窃走。Polo Ralph Lauren 条信息泄露事件危及多达 180,000 人的信用卡数据安全。[10]

英国一家第三方投资管理公司 Capita Financial Administrators Limited (CFA) 曾发现客户信息已经被更改，而且对客户帐户做了欺骗性付款请求。这些交易在同谋的 CFA 职员帮助下进行，100 多万英镑的请求被监测到并予以制止，但是之前已有 300,000 多英镑的欺骗性付款得逞。随后英国金融服务管理局 (Financial Services Authority, FSA) 因该公司防欺诈系统和控制的失效而对其罚款 300,000 英镑。[11]

何为对数据隐私的内部威胁？

当许多公司花费大量的时间和资金来保护自己的系统免于外部攻击时，它们并没有意识到 70% 的数据泄露源于内部！[12]

客户数据特别容易由内部泄露——无论犯人是不满的雇员还是粗心的服务提供商。许多公司可能牢牢地锁定了主处理系统，但敏感数据还存在于许多其他地方。部署、测试、备份、质量控制和培训等非生产环境是特别薄弱的环节。例如，如果内部开发和质量保障职员负责交付新的和增强的业务应用，他需要访问实际的测试数据。通常，这种数据从生产环境复制，用于非生产数据库。这种惯例开放了许多内部数据泄露的可能，从而导致可不受限制地访问机密客户信息以及公司内部财务和人力资源信息。

此外，外包应用程序开发和测试活动已经非常普遍。一旦您在外包位置或海外创建了用于非生产环境的生产数据副本，就更难控制可访问机密消费者信息的人员了。

最后，在受保护的位置之外能够存储或管理机密信息的笔记本电脑和其他便携式设备提高了脆弱性程度。含有敏感数据的笔记本电脑、USB 设备或其他类型介质丢失数据的现象已极为普遍。例如，英国国家建筑协会(Nationwide Building Society)是英国最大的建筑业组织，在其雇员的笔记本电脑于家中失窃后被罚款 980,000 英镑。该笔记本电脑包含建筑协会近 1100 万客户的姓名、地址和帐号，这些客户暴露在金融犯罪的风险之中。[13] 类似情况有，包含 2650 万退伍军人及其家庭的数据从就职于美国退伍军人部（US Department of Veterans Affairs）的员工家里被偷走。

为什么这些非生产环节如此脆弱？

与开发、测试和培训环境一样，非生产环境是受欢迎的攻击目标。为什么？因为，在防火墙、加密和网络安全等生产系统中保护数据的手段一般不会同样适用于非生产环境。为了开发或测试应用，您的职员必须使用不违反应用逻辑的、准确、实际的数据。

来自生产系统的真实客户数据满足这种要求，但暴露这些信息危及了隐私的安全。更重要的是，使用生产数据进行测试的这些公司违反了 PCI DSS 的要求 6 和 7（参见表 2）。这些要求限制访问和利用持卡人数据信息。

表 2. PCI 要求 6 和 7

开发并维护安全的系统和应用
6.3——根据行业最佳实践开发软件应用程序，并在整个软件开发生命周期内实现信息安全。
6.3.4——生产数据（现场 PAN）不得用于测试或开发[PANs 个人帐号]
按照“按需知道”的原则严格限制对持卡人数据信息的访问
7.1 ——限制访问计算资源和持卡人信息，只对工作需要这种访问的个人开放。

开发人员和质量保证人员不需要访问“真实的”持卡人数据信息。相比之下，他们需要逼真的、上下文关系准确的数据，这些数据模拟存储在应用数据库中的信息，却不危及隐私。最终，贸易商需要屏蔽机密数据的功能，使之安全地用于应用程序开发测试。

保护消费者数据的最佳方式是什么？

行业分析师同意，当将数据从生产环境迁移到测试或其他非生产环境中时，保护机密数据的有效解决方案就是应用去标识化技术。去标识化是系统屏蔽或转换社会保障号码、银行帐号、出生日期和地址等个人可标识信息（Personally Identifiable Information，PII）的过程。

以这种方式被清理过的数据可以用于测试。

数据去标识化使开发人员和测试人员使用逼真的测试数据并生成有效测试结果，同时遵守了 PCI DSS。但重要的是要注意数据转换的结果必须适合应用的上下文。也就是，数据转换的结果必须尊重应用的业务逻辑。

例如，含有字母字符的数据应该用其他字母字符以适当的方式代替。此外，经过转换的数据必须在允许值范围内。

除了提供数种屏蔽或去标识化复杂关系数据的方式外，一个有效的解决方案还应支持多种应用、数据库、操作系统和硬件平台。简言之，您需要一种能伸缩的解决方案来满足当前和未来的需求。

IBM Optim 支持您的 PCI 遵从举措

IBM® Optim™ Data Privacy Solution 为您提供久经考验的技术，允许组织使用相关测试数据的参考性完整子集来创建、屏蔽并维护逼真而合适的测试数据库。

Optim 提供了多种数据转换算法和内建的查找表格，甚至支持自定义数据屏蔽例程。Optim 生成上下文准确且应用可感知的屏蔽数据。

IT 职员可以利用 Optim 生成有效的经过屏蔽的数值，用作支付卡号、国别标识符、姓名和其他形式的 PII。屏蔽数据不仅可呈现对盗窃者无用的卡信息，而且能遵守 PCI DSS 要求 6 和 7。此外，所屏蔽的数据元素可以跨相关表格传播，以确保数据库的参考完整性。

Optim 支持领先的数据库管理系统，并向开发人员提供能够在单一流程中从各种数据源提取和屏蔽适当测试数据的联邦身份访问功能。Optim 能够满足您当前的需求并能轻松适应您 IT 环境中的各种变化。除了帮助您满足各种遵从性举措，Optim 的功能还可帮助您减少在整个应用生命周期内与开发和测试相关的时间和成本。

由于零售商拥有的客户数据量大且敏感，所以他们是黑客和类似的数据盗窃者的攻击目标。“遵循‘保护客户数据然后证明遵从性’的理念，而非首末倒置地，在 PCI 遵从性方面的支出必须以最重要的关键业务风险为目标。”[14]

PCI DSS 规定了 12 条保护支付卡客户的要求。在屏蔽机密数据和确保机密数据可为工作需要的个人所使用方面，这些要求非常明确。使用综合数据屏蔽功能，您能去标识化支付卡号以及其他 PII，IBM Optim 能帮助您在非生产（开发、测试和培训）环境中保护您的机密客户信息，以符合 PCI DSS 的要求。

关于 IBM Optim

IBM® Optim™ 企业数据管理解决方案关注关键的业务问题，例如，数据增长管理、数据隐私遵从性、测试数据管理、电子发现、应用升级、迁移和退役。

Optim 使应用数据管理适应业务目标，以帮助优化性能、降低风险并控制成本，同时提供跨企业应用、数据库和平台进行伸缩的功能。

如今，Optim 帮助全球所有行业的企业利用在企业应用数据生命周期的每个阶段管理其数据的能力，充分发挥了企业应用和数据库的商业价值。

更多信息

要了解 IBM Optim 企业数据管理解决方案的更多信息，请与 IBM 销售代表联系，或者访问：http://www-01.ibm.com/software/cn/data/data-management/optim-solutions/。

IBM Software Group

111 Campus

Drive Princeton, NJ
USA,
08540-6400

800.457.7060
609.627.5500

传真 609.627.7799

www.optimsolution.com

在美国印刷

2008 年 3 月

[1] *CJ Writer， "Credit Cards: What You Need to Know to Avoid Getting Hurt Financially，" Associated Content，associatedcontent.com，2006 年 3 月 16 日。*

[2] *Grainne Gilmore， "Credit card spend sounds credit crunch alarm，" http://business.timesonline.co.uk/tol/business/money/borrowing/ article3368934.ece，2008 年 2 月 14 日。*

[3] *"A Chronology of Data Breaches，" Privacy Rights Clearinghouse，2008 年 3 月 17 日更新，www.privacyrights.org*

[4] *Noel Yuhanna， "Enterprise Databases Need Greater Focus to Meet Regulatory Compliance Requirements，" Forrester Best Practices，2007 年 1 月 24 日。*

[5] *"2006 Privacy Trust Study for Retail Banking，" The Ponemon Institute，LLC and Vontu，Inc.，2006 年 1 月，as referenced in "Ponemon Institute Names Most Trusted Retail Banks，" Vontu Press Release，2006 年 1 月 26 日。*

[6] *"Identity Fraud is Dropping, Continued Vigilance Necessary，" Javelin Strategy & Research，2007 Identity Fraud Survey Report，2007 年 2 月，as referenced by Jonathan Stempel， "U.S. Identity theft losses fall: study，" Reuters，2007 年 2 月 1 日。*

[7] *Jaikumar Vijayan， "TJX breach uncovers security holes，wrong practices in retail industry，" Computerworld (US online)，2007 年 1 月 22 日。*

[8] *Paul F. Roberts， "Retailer TJX reports massive data breach，" Infoworld.com，2007 年 1 月 17 日。*

[9] *Thomas Claburn， "BJ's Wholesale Club Settles FTC Data-Protection Complaint，" Information Week.com，2005 年 6 月 16 日。*

[10] *Alorie Gilbert， "Retailers feel security heat，" CNET News.com，2005 年 4 月 22 日。*

[11] *"FSA fines Capita Financial Administrators Limited £300,000 in first anti-fraud controls case，" Financial Services Authority，FSA/ pn/019/2006，2006 年 3 月 16 日。*

[12] *Richard Mogul， "Danger Within——Protecting your Company from Internal Security Attacks，" Gartner，2002 年 8 月。*

[13] *"Nationwide fine for stolen laptop，" BBC News，News .bbc. co.uk，2007 年 2 月 14 日。*

[14] *Avivah Litan 和 John Pescatore， "Answers to Common Questions about PCI Compliance，" Gartner Research，ID Number G00144907，2006 年 12 月 7 日。*

IME14000-USEN-00