



---

## 确保电子支付的安全

---

信任是电子支付行业成功的关键。这也是长期以来为什么 Visa 在开发数据安全解决方案领域方面始终保持领先地位的原因。

### 设立数据安全标准

Visa 是最早着手解决新兴的信息安全问题的行业领袖。早在 2000 年，Visa 就建立推出了持卡人信息安全计划 ( Cardholder Information Security Program, CISP ) ——也是第一个全球范围内保护持卡人敏感信息的数据安全标准。持卡人信息安全计划后来成为行业安全标准，适用于所有从事持卡人敏感数据储存、处理、传输的相关机构。

2004 年，Visa 和其他主要支付品牌达成一致，同意共同制定一个全球通用的安全标准，即支付卡行业数据安全标准 ( Payment Card Industry Data Security Standard, PCI DSS ) ，从而扩大了整个行业对于支付安全标准的接受范围，加强了对持卡人数据的保护。

### 积极加强安全标准合规工作

尽管支付行业安全标准是由 PCI 安全标准委员会进行管理的，但是，该标准的实施却取决于各支付卡组织的推动力度。而 Visa 一直将不断推进支付安全标准这一工作为己任，予以认真贯彻和执行。

2006 年，Visa 推出了 Visa PCI 加速合规计划 ( PCI CAP ) ，该计划提供 2,000 万美元的奖励资金，用于奖励符合 PCI 安全标准的商户。该项目是第一个对支付行业一直以来的、单一的处罚措施的一种有效补充。该项目还制定了严厉的处罚措施，其中包括对违规储存某些敏感数据和没有完全达到 PCI 标准要求的商户进行罚款。通过推出这种创新计划，Visa 成为行业第一家将交换费与安全性挂起钩来的企业，即只对达标商户的交易提供优惠。

该计划推出后，大型商户 ( 一级 ) 的合规率达到了 36%，中型商户 ( 二级 ) 的合规率达到了 15%。而 Visa 一半以上的收入来自一级和二级商户。为了鼓励收单机构和商户尽快合规，Visa 将 2007 年 9 月 30 日设为一级商户合规的最后期限。该截止日期之后，Visa 开始对其美国收单机构采取处罚措施，即如果收单机构有一个未达标的商户，那么，它将每月被罚款 25,000 美元。自从该计划实施以来，达标率快速提升。迄今，超过 99% 的一级和二级商户已经确认它们没有储存敏感数据，从而最大程度降低了支付系统数据的一个重大风险。

Visa 还一直积极鼓励小型商户实现 PCI DSS 达标。2007 年 5 月，Visa 要求其美国收单机构对小型商户的数据安全风险进行调查，并开展相关教育活动，使商户进一步关注并了解数据安全和 PCI DSS 安全标准对于它们业务的重要意义。自 Visa 提出该项要求之后，美国目前所有收单机构都已向 Visa 提交了方案，并且正在实施各自的安全计划。

### **开发工具以支持合规——聚焦支付软件**

除了通过奖罚措施鼓励合规之外，Visa 还努力开发有助于提高支付环境安全性的工具和支付软件，以加强合规工作。2005 年，Visa 开展了“支付应用最佳案例”（Payment Application Best Practices, PABP）项目，帮助软件厂商开发安全支付应用软件。司法机构在对数据泄露进行的调查中发现，某些支付应用建立于储存违禁数据的基础之上，因此给它们的用户带来了安全漏洞。为了更好地保护持卡人信息，Visa 宣布了要求商户只使用不储存敏感数据的支付系统软件的计划。

2007 年下半年，PCI 安全标准委员会对 Visa 在支付安全领域的领先性表示了认可，并决定采用 Visa 的“支付应用最佳案例”作为支付行业内新的第三方应用软件安全标准——并将其称为“支付应用数据安全标准”（Payment Application Data Security Standard, 即 PA-DSS）。

### **提供广泛的教育资源**

作为数据安全的倡导者和领先者，Visa 还面向商户、收单机构、卡信息处理机构和支付应用供应商开展了多种教育活动。Visa 的在线教育中心（网址：[www.visa.com/cisp](http://www.visa.com/cisp)）提供了多种网络会议、安全警示和培训课程，能够帮助商户更好地了解 PCI DSS 的内容以及合规要求。

Visa 还积极与各知名企业合作，推广这些教育项目。在 2005 年-2006 年期间，Visa 联合了美国商会开展了覆盖 21 个城市的商户数据安全巡展，涉及 60,000 家小型商户。2007 年，Visa 联合全美独立工商业者联合会（NFIB）开展了针对小型商户的数据安全培训，并且编写了《NFIB 数据安全指南》——一本专为 NFIB 的 35,000 个小型商户成员编写的手册。Visa 还参与了优良企业局理事会的《使这一切变得更简单（MADE SIMPLER）》的编写，并与金融机构合作，将该手册分发给全球各地的小型企业持卡人和受理支付卡的小型商户。

对于 Visa 而言，没有任何一件事比维护其支付系统的安全更为重要。Visa 目前所做的一切努力已经帮助公司降低了欺诈率，这也是 Visa 能够成为支付安全领域的全球领袖之一的的原因。

## **VISA数据安全达标重大事件**

### **2000 年**

Visa 提出持卡人信息安全计划（CISP）——第一套用于在全球范围内保护敏感持卡人数据的标准。

### **2001 年**

CISP 成为所有储存、处理或传输敏感 Visa 持卡人数据的机构必须遵守的标准。2001 年在东京召开

的西方八国集团打击高科技犯罪会议所发布的最佳实践就是以CISP要求为蓝本。

#### **2004 年**

Visa的CISP数据安全要求为支付卡行业数据安全标准 ( PCI DSS ) 奠定了基础，PCI DSS提供了一套行业通用的工具和指标，有助于确保敏感持卡人信息的安全处理。

#### **2005 年**

Visa推出“支付应用最佳案例“ ( PABP ) ，帮助软件厂商开发安全支付应用，从而确保它们的客户达到PCI DSS要求，避免数据安全的问题。

#### **2006 年**

Visa启动了致富行业数据安全标准合规加速计划 ( PCI CAP ) ，共拨款项 2,000 万美元作为奖励资金，同时，制定了新的处罚措施，旨在进一步推进商户遵从PCI DSS这一标准。该计划也是对支付行业过去一个时期的单一处罚措施的一种有效补充。

Visa 成为全球第一家公布 PCI DSS 合规率的公司：

- 一级商户：36%
- 二级商户：15%

#### **2007 年**

7 月——Visa宣布推出了一个旨在帮助美国小型商户改善数据安全的计划。Visa的计划要求收单机构查明并解决它们的小型商户所面临的数据泄漏风险，其中包括查明该商户是否储存敏感账户数据和是否遵守PCI DSS的数据安全标准。

7 月——Visa宣布，受理Visa卡的大型商户 ( 一级和二级商户 ) 中已有 96%确认它们没有储存敏感数据。Visa成为第一家对储存敏感数据的商户进行罚款的银行卡机构。Visa更新PCI DSS达标率：

- 一级商户：40%
- 二级商户：33%

10 月——，Visa 开始对其美国收单机构实施处罚措施，前提是：如果收单机构有任何一家一级商户在规定的截止日期 ( 2008 年 9 月 30 日 ) 前仍未达到 PCI DSS 标准的合规要求，那么，这家收单机构将被处罚每月 25,000 美元的罚款。Visa 也因此成为第一家针对没有合规的机构处以罚款的卡组织。

10 月——Visa 更新 PCI DSS 达标率：

- 一级商户：65%
- 二级商户：43%

11 月——PCI 安全标准委员会采用 Visa 率先发布的“支付应用最佳案例“作为支付行业的新的第三方应用软件安全标准。这个新的行业标准被命名为“支付应用数据安全标准” ( PA-DSS ) 。

11 月——Visa 提出了一系列要求，规定其美国商户及其代理商使用不储存敏感卡信息的支付系统软件。这些要求旨在保护持卡人信息和完善其它安全措施，其中包括 PCI DSS 合规。

12 月——Visa 更新 PCI DSS 达标率：

- 一级商户：77%
- 二级商户：62%

-- 完 --