支付卡行业的未来：
任世界纷繁变幻 为支付保驾护航

Jeremy King
2014年

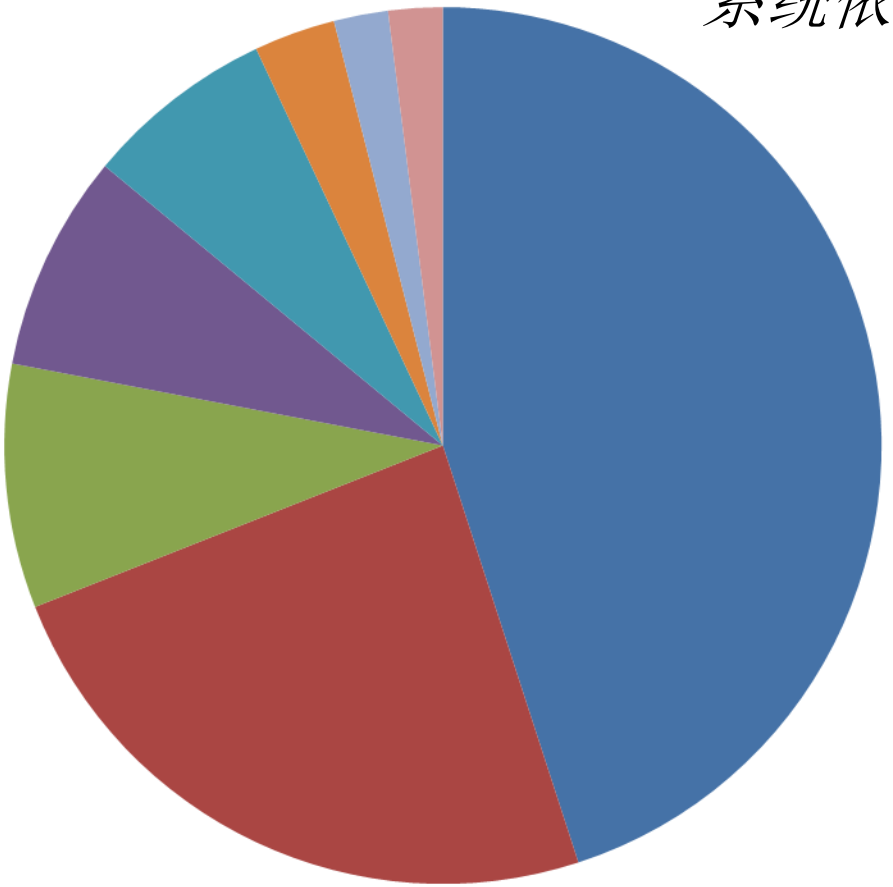
PCI Security Standards Council

卡片数据是犯罪分子的金矿

支付卡上的数据类型

数据泄露高发行业

存储、处理或传输持卡人数据的系统依然是犯罪分子的主要目标



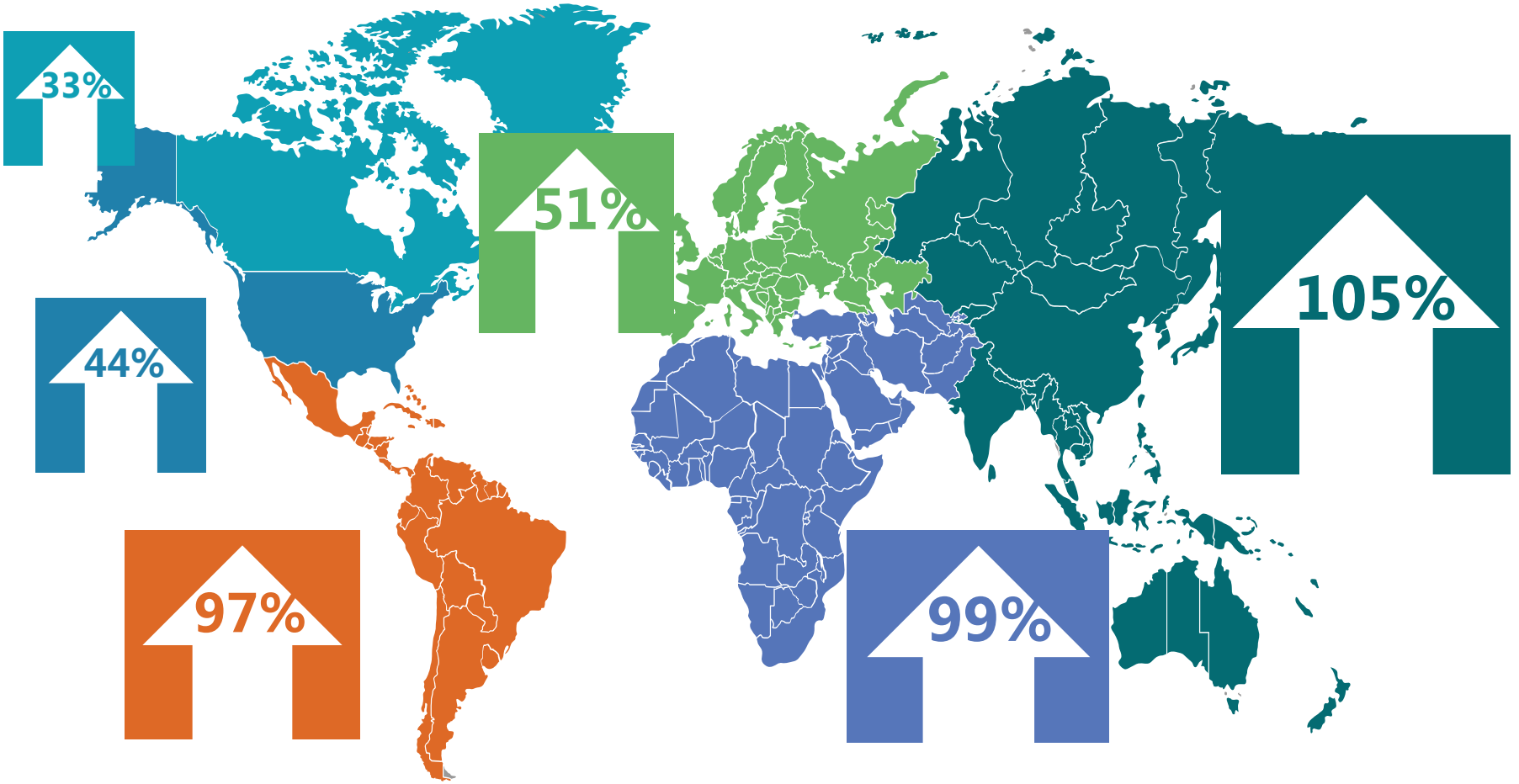
资料来源：Trustwave公司2013年全球安全报告

谁是高风险群体？


Sm.$2.75
WILD Med.
WILD Lg.
Homemade yogurt,
with granola & up
GPM
Dividends
41%
67,228,166
13,946,511
6,504,606
1,960,477
7,736,223
5,825,769
35,973,586
31,254,580
3,599,566
27,655,014
Loans
Shares

大多数内部泄露由支付链中的人造成！

随着全球卡片使用量的增加，风险也在增加



2011至2016年全球刷卡交易增长率

司法审计暴露出的频发错误

密码安全级别低或使用默认密码

******

缺乏对员工的教育培训

第三方机构造成的安全缺陷

缺乏自我检测

资料来源：Trustwave公司2013年全球安全报告

高级密码不需要那么复杂

密码	破解时间
bigmac	0.077秒 （非字典词汇）
B1gMac	14秒（大写字母，小写字母，数字）
B1gMac1	14分钟 （7个字符）
leB1gMac	15小时 （8个字符）
B1gMac399	39天 （9个字符）
B1gMacfries	412 年 （11个字符）
Bigmacandfries	511 年 （ 14个字符，但只有字母）
B1gMac&fries	344,000年（12个字符）

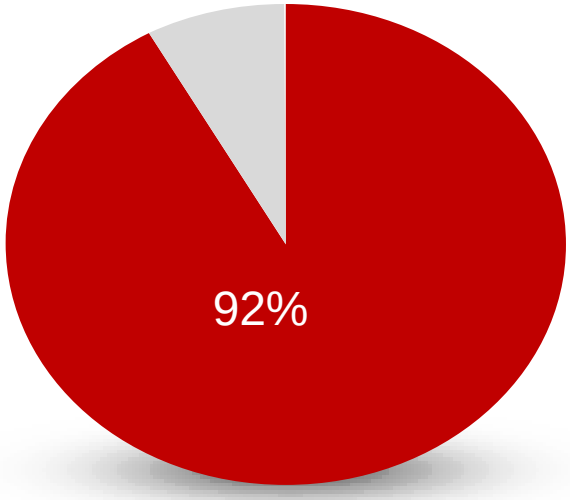
2013*年25个最常见的密码

1. 123456 (上移1位)
2. password (下移1位)
3. 12345678 (不变)
4. qwerty (上移1位)
5. abc123 (下移1位1)
6. 123456789 (新增)
7. 111111 (上移2位)
8. 1234567 (上移5位)
9. iloveyou (上移2位)
10. adobe123 (新增)
11. 123123 (上移5位)
12. admin (新增)
13. 1234567890 (新增)
14. letmein (下移7位)
15. photoshop (新增)
16. 1234 (新增)
17. monkey (下移11位)
18. shadow (不变)
19. sunshine (下移5位)
20. 12345 (新增)
21. password1 (上移4位)
22. princess (新增)
23. azerty (新增)
24. trustno1 (下移12位)
25. 000000 (新增)

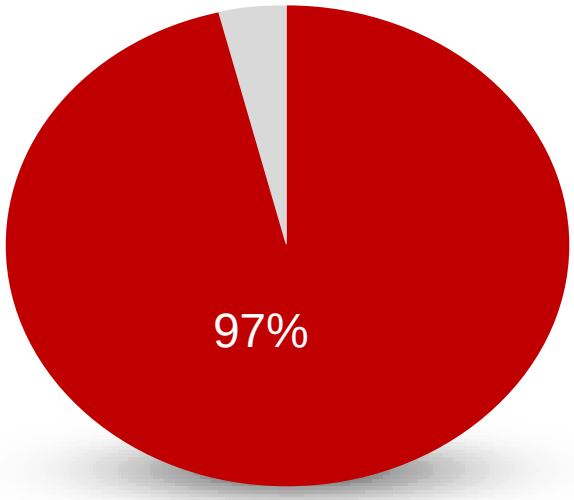
* CBS新闻，2014年1月21日

支付卡行业标准 维护数据安全

92%的泄露案件采用简单方法



97% 的泄露案件通过简单或中等力度的控制措施可以避免



资料来源：Verizon2012数据泄露调查报告

忽视支付卡行业标准的机构往往受到攻击

截至最后一次评估，96%的被攻击机构未遵守支付卡行业标准（或从未接受评估/验证）

攻击机构的方法：

- 81% 为黑客攻击
- 69%为恶意软件入侵
- 10%为物理攻击

资料来源：Verizon2012数据泄露调查报告

为何？

为何我们无法营造安全的环境

- IT从业者缺乏安全意识
- 缺乏将安全作为重中之重的激励措施
- 技术发展日新月异
- 新解决方案开发快、分布广
- 持卡人数据仍出现不必要的暴露

支付卡行业：支付卡安全架构

五大卡片品牌努力推动支付卡安全

支付卡行业安全标准委员会管理技术标准和流程

支付卡行业委员会简介

开放的全球论坛

2006年成立

引领支付卡安全公开标准

- 重发展
- 重管理
- 重教育
- 重观念

扩大全球影响力

支付卡行业委员会的顾问委员会

支付卡行业安全标准组合

保护持卡人支付数据

打造支付设备、程序、基础设施和用户的生态系统

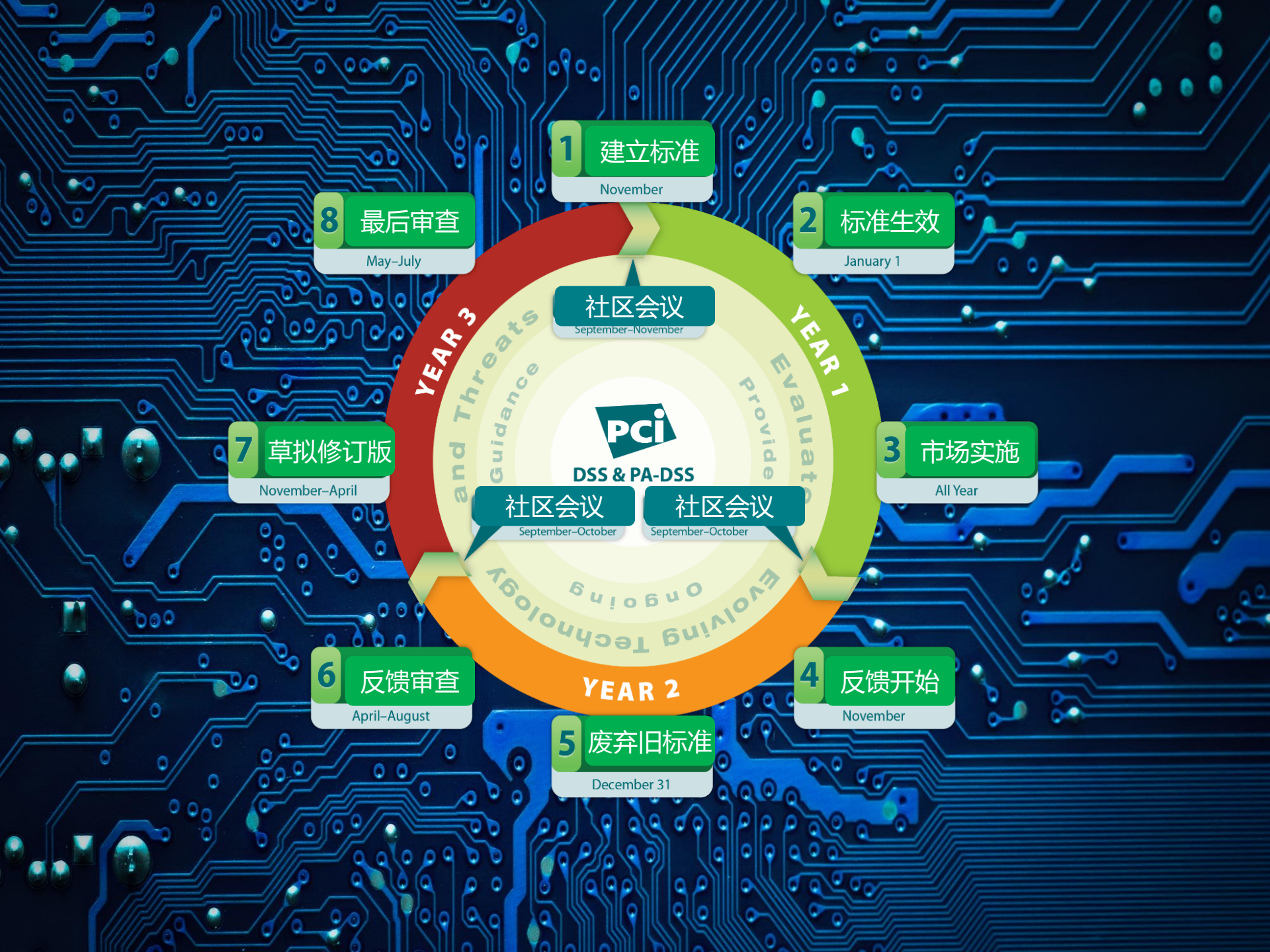
支付卡行业标准 维护数据安全

90%的安全专家都推荐支付卡行业标准

来源：安全报告的真实成本，第451组

采纳支付卡行业数据安全标准的大型机构，其安全控制措施更加完备。这些机构的数据不容易被盗取。

资料来源：Trustwave公司2013年全球安全报告


1 建立标准
November
2 标准生效
January 1
3 市场实施
All Year
4 反馈开始
November
5 废弃旧标准
December 31
6 反馈审查
April–August
7 草拟修订版
November–April
8 最后审查
May–July
社区会议
September–November
社区会议
September–October
社区会议
September–October
YEAR 1
YEAR 2
YEAR 3
Evaluate
Provide
Ongoing
Evolving Technology
Guidance
and Threats
PCI
DSS & PA-DSS

支付卡行业数据安全标准（PCI DSS）
支付程序数据安全标准（PA-DSS 3.0）

PCI Security Standards Council

引领全球支付卡安全公开标准

标准初探……

- 支付卡行业数据安全标准（PCI DSS）的12条核心安全原则保持不变
- 影响支付卡行业数据安全标准制定工作的子需求
- 重大变革即将实施的日期
- 支付卡行业数据安全标准的适用性清晰明了
- 测试程序增强，明晰每项需求所需的验证水平
- 需求和测试程序使用相同的语言
- 合规性报告（ROC）说明现在与ROC报告模板分开

POS设备的物理安全性

9.9 保护读取支付卡数据的设备，防止数据篡改和替代

- 运用最新设备清单
- 定期检查设备表面，检测篡改或替换情况
- 培训相关人员，防止篡改数据或更换设备

渗透测试与有效审视

11.3　采用渗透测试方法

11.3.4 若采用细分方法，请进行渗透测试，证明细分方法是可操作的有效方法。

安全是共同的责任

指导	• 支付卡行业数据安全标准（PCI DSS）责任外包
第8.5.1项要求	• 可以访问用户环境的服务提供商，使用与每位客户对应的唯一身份验证凭据
第12.9项要求	• 第12.8条附属条款；处理或管理客户持卡人数据的服务提供商必须声明其遵守支付卡行业数据安全标准的要求。

支付卡行业成功的秘诀

支付技术

移动设备

点对点加密

虚拟化

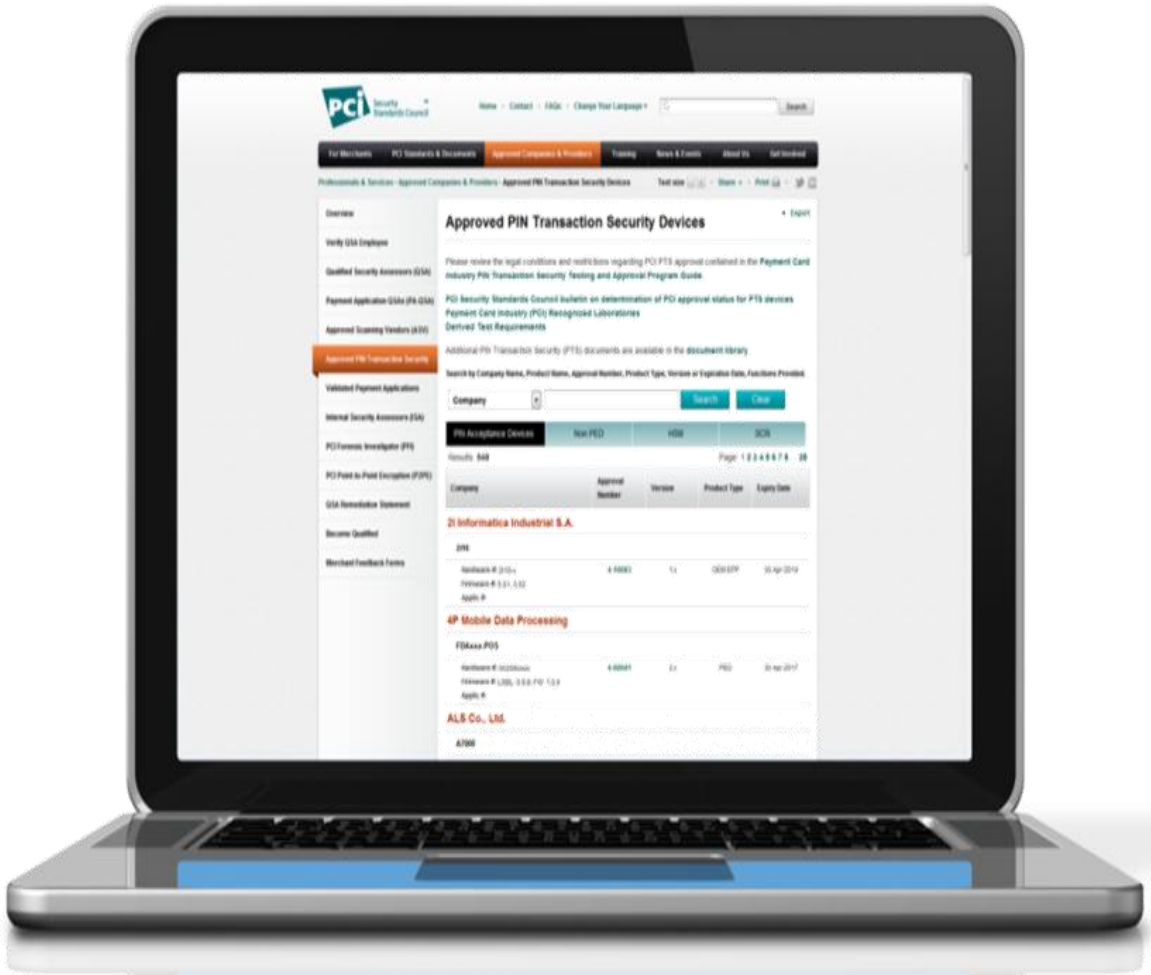
无线网

标记化

基于电话的
支付卡数据

EMV芯片

EMV芯片 + 支付卡行业（PCI）共同为安全保驾护航



PCI Security Standards Council

EMV芯片可以有效减少面对面欺诈

EMV芯片需要支付卡行业（PCI）

点对点加密

公司	验证	点对点加密顾问	再次验证日 受理日起一年后	到期日 受理日起两年
欧洲支付业务有限公司				
EPS Total Care P2PE				
Version #: 13-02.00869.001	Validated According	SecurityMetrics,	2014年10月18日	2015年10月18日
Logic集团				
Solve DataShield P2PE Solution for Ingenico				
Version #: 13-02.00830.002	Validated According	Foregenix	2014年11月20日	2015年11月20日

制定标记化技术标准的工作已经展开

卡号

移动设备

支付卡行业标准聚焦商户受理范围

移动支付受理范围还有待扩大

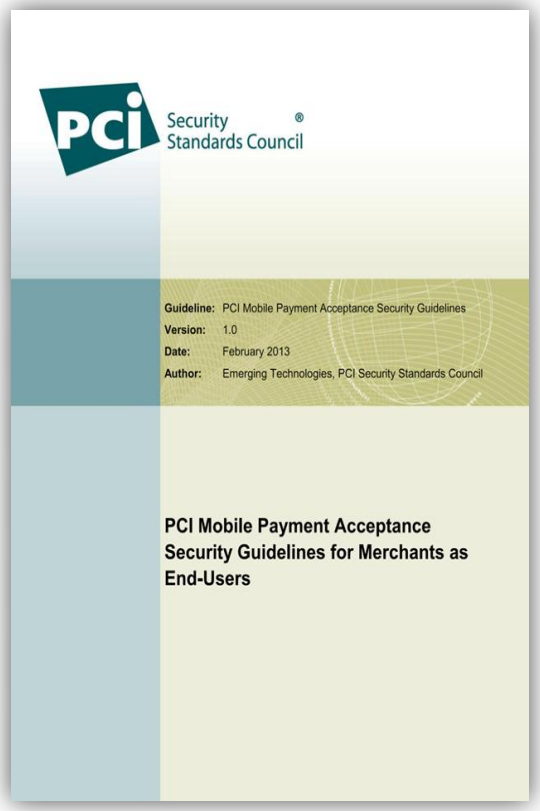
了解风险
运用支付卡行业安全标准委员会资源

支付卡行业安全标准委员会与业界通力合作

移动支付准则与最佳实践

2012-2013年公布的准则

- 针对开发人员的支付卡行业移动支付受理准则
- 针对终端用户商户的支付卡行业移动支付受理准则
- 用智能机或平板电脑受理移动支付



支付卡行业特殊利益集团（PCI SIG）指导文件

云端

电子商务

标记化

访问www.pcisecuritystandards.org
下载该准则

特殊利益集团（SIG）

保持支付卡行业数据安全标准的合规性

183个成员

第三方安全保证

196 个成员

支付卡行业官网提供多语言版本

- 中文
- 法语
- 德语
- 日语
- 意大利语
- 葡萄牙语
- 俄语
- 西班牙语

热门培训

- ✓ 网上内部安全评估员（ISA）培训
- ✓ 点对点加密评估员培训
- ✓ 支付卡行业企业认知培训——让我们为您服务！
- ✓ 四小时认知在线培训
- ✓ 合格集成商和经销商（QIR）™ 计划
- ✓ 支付卡行业专家计划（PCIP）™

欲了解更多信息，请访问：
www.pcisecuritystandards.org/training

内部安全评估员（ISA）计划

为合格内部审计安全专家推出的，支付卡行业数据安全标准全面培训和资格评定计划！

- 增强对支付卡行业数据安全标准和合规程序的了解
- 帮助机构培养内部专业技能
- 教授流程，降低合规成本

支付卡行业认知培训

团队建设

便捷

实惠

我们欢迎您的加入！

PCI Security Standards Council

引领全球支付卡安全公开标准

合格集成商和经销商（QIR）™

合格集成商和经销商（QIR）帮您走出常见误区

我使用的是经支付程序数据安全标准（PA-DSS）验证过的程序，肯定没问题。

我使用的是“有信誉”的第三方机构，安装肯定安全放心。

该问题只适用于实体企业。

支付卡行业专家计划（PCIP）™

现已推出

PCI Security Standards Council

引领全球支付卡安全公开标准

为未来做好准备

应对新型威胁，加强支付卡行业的个人培训至关重要

委员会开展的支付卡行业培训是提升专业技能、紧跟行业潮流最有效、最具针对性的培训

通过验证将向雇主证明您的价值，同时让您从所谓的“专家”中脱颖而出

关注日期 静待开幕—— 2014年区域会议

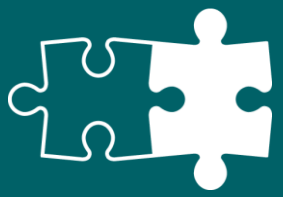
北美	欧洲	亚太
		
9月9-11 日 佛罗里达奥兰多	10月7-9 日 德国柏林	11月18-19 日 澳大利亚悉尼

脱颖而出——成为参与机构

成为参与机构（PO）的益处：

- 两张区域会议免费门票
- 参加委员会培训享受优惠价格
- 有权选举顾问委员会委员
- 有机会参与特殊利益集团
- 更多好处 等你体验！

快快参与——我们需要您注入新鲜血液



参与

学习

奉献

网络

提名

选举

分享

影响

问题？

安全标准委员会

请访问我们的官网： **www.pcisecuritystandards.org**