



## Payment Card Industry (PCI) Compliance

*Stronger standards, better protection*

**Vinu Thomas**

---

What would happen to your company's reputation, customer confidence and future revenues/profits if your business had to issue a letter to your customers similar to this one?

Dear \_\_\_\_\_:

*We are contacting you about a potential problem involving identity theft. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts.*

Identity theft and credit card fraud are serious and growing threats to consumers. Last year, the U.S. Treasury Department reported that cybercrime proceeds outstripped those of illegal drug sales, netting an estimated \$105 billion. 80 million data records of U.S. citizens have been exposed due to various security breaches since 2005. Many more incidents are likely to go unreported to avoid the blow to a company's credibility. Reported incidents may be only the tip of the iceberg. Cybercrime is big business and it's getting bigger, better organized, and more sophisticated. For example, the information associated with a single credit card number is worth \$100, or more, on the black market in places such as Eastern Europe. That provides a lot of incentive to someone capable of exploiting the holes and vulnerabilities in your organization's IT infrastructure.

To ensure that your business will never have to say, "we're sorry", major credit card providers have collaborated to develop the Payment Card Industry (PCI) Data Security Standard. For the first time, security requirements and standards for all card types align with one standard. Merchants and service providers who store, transmit, or process credit card transactions must comply with this standard or they will lose the ability to conduct business with the leading credit card companies.

All major credit card associations including Visa, MasterCard, American Express, Discover, Diners Club and JCB endorse, and require the unified PCI Data Security Standards. Failure to comply can result in permanent prohibition of the merchants or service providers' participation in credit card processing programs and a fine. Liability payouts for fraud will shift from the card associations to the merchants that are in non-compliance compliance. Additionally, Mastercard and Visa may impose fines of up to \$500,000 per incident.

*Knowledge. Experience. Results.*



STRATEGIC COMPUTER SOLUTIONS

**These mandated standards require an organization to:**

- Install and maintain a firewall configuration to protect data
- Avoid the use of vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data and sensitive information across public networks
- Deploy and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Regularly track, monitor, and test all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a comprehensive information security policy

Unlike government regulations such as HIPPA and Sarbanes-Oxley, PCI Compliance is not yet mandated. This has resulted in a slow adoption rate but the credit card companies, themselves, have added the teeth to the standards through fines and disallowing companies to use their cards online to conduct transactions. Visa reports that 22% of their Tier 1 merchants (those processing more than 6 million credit card transactions per month) are fully compliant. Slowly, but surely, the remaining 78% are moving in that direction.

When choosing a certified consultant to help your business achieve PCI compliance, it's important to determine that they have the skills and experience to conduct a full network assessment including all external connections into the network (e.g. employee remote access, payment card company, third party access for processing, and maintenance); all connections to and from the authorization and settlement environment; and, any data repositories. Compliance status must be reviewed annually by merchants of all sizes. In the not-too-distant future, customers may avoid any online transactions in venues that do not meet the PCI Standards. Although it may be a few years before the PCI Standards show their teeth, your business can avoid losses and fines, and reap the rewards of customer confidence by achieving compliance sooner, rather than later.

We are pleased to announce that Strategic Computer Solutions has achieved the status of a Payment Card Industry (PCI) Compliance Vendor, joining a select group of companies in the world to be able to offer this service to our customers.

MasterCard and Visa, in the US and Europe, have evaluated SCS Security & Networking processes and procedures, conducted interviews with SCS personnel, and reviewed security assessments, and they have now given SCS the authorization to certify a business as PCI compliant, perform external audits, review existing policies and procedures, and also provide remedial solutions, technology and services to meet the stringent PCI Data Security Standards.



STRATEGIC COMPUTER SOLUTIONS

[www.scsinet.com](http://www.scsinet.com)

**Vinu Thomas,**

CISSP, Chief Security Architect

Tel: 973.731.1464

[vthomas@scsinet.com](mailto:vthomas@scsinet.com)

