



February 13, 2008

PCI Compliance: What it Means to the Call Center Industry

By [Christopher M. Carrington](#)
CEO, Alpine Access

It seems we read about it on a daily basis. Large scale security breaches have happened to some of the most well-known companies in the world, and they can happen to you. Hackers are finding new ways to collect massive amounts of consumer data and companies that inadvertently let this happen are paying for it — literally. Take TJX Companies, for example, the parent organization for T.J. Maxx and Marshalls. This company recently paid millions of dollars to settle a class action lawsuit for allowing one of the largest data breaches in history — 94 million credit card records over three years.

Dai Nippon Printing, SAIC, GAP and the Department of Veteran Affairs to name a few, all experienced large data breaches in 2007. As networks become more complex and thieves get smarter, protecting cardholder information is more important than ever. In response to an undeniable need for security education, direction and guidelines, the five major credit card brands (MasterCard, VISA, AMEX, DiscoverCard & JCB International) joined forces in September 2006 to create a standard for protecting cardholder information. Known as the PCI Data Security Standard (PCI DSS), this major compliance initiative details the steps needed to minimize the potential for fraud and reduce system exposure. A combination of security policies, technology and network changes, this standard is now mandatory for any merchant who accepts, captures, stores, transmits, or processes credit and debit card data. Companies not in compliance can face fines between \$5,000–\$25,000 a month. In a corporate press release, Visa reported imposing \$4.6 million worth of fines for non-compliance in 2006.

In my opinion, PCI compliance is a smart business decision, especially for call centers that regularly handle financial transactions. It provides confidence to clients and partners that their data is protected in the best possible way. Yet, despite all the evidence in favor of implementing strong security measures, there are still many organizations that have decided not to pursue compliance or have elected to meet just the bare minimum requirements. When selecting an outsourcing call center partner, companies must understand the level of certification, and thereby the level of protection, the call center provides them. It is also important to remember that

certification is an ongoing process. Companies that claim PCI compliance at one point in time need to provide proof of established processes that will maintain compliance over the years.

PCI Certification

For a company to say it is PCI compliant it must prove that its infrastructure meets 12 major requirements broken into six sections called “control objectives.” While each of these areas has numerous actions associated with it, the main objectives and requirements are as follows:

- Build and Maintain a Secure Network
 - Install and maintain a firewall configuration to protect data
 - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
 - Protect stored cardholder data
 - Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
 - Use and regularly update antivirus software
 - Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
 - Restrict access to cardholder data by business need-to-know
 - Assign a unique ID to each person with computer access
 - Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
 - Track and monitor all access to network resources and cardholder data
 - Regularly test security systems and processes
- Maintain an Information Security Policy
 - Maintain a policy that addresses information security

To validate compliance, a Qualified Security Assessor (QSA) performs an audit. The amount of detail involved in this audit, or the number of specific criteria analyzed, depends on the type of merchant. While each credit card company has its own criteria for categorizing merchants, in general, the merchant level is based on the number of transactions performed. Obviously, the higher the transaction volume, the more data is at risk and, consequently, the more stringent the criteria are for obtaining certification.

The current merchant levels for VISA and MasterCard are:

- Level 1 – companies with transactions totaling 6 million and greater, per year.
- Level 2 – companies with transactions totaling 1–6 million, per year.
- Level 3 – companies with transactions totaling 20,000–1 million per year.
- Level 4 – companies with transactions totaling up to 20,000 per year.

To validate PCI compliance, Level 1 merchants must complete an annual onsite audit by a QSA and quarterly network security scans with an Approved Scanning Vendor (ASV). Level 2 and Level 3 merchants, in contrast, need only to complete a self assessment questionnaire along with the quarterly network scans. The difference in the amount of time and financial investment required for Level 1 versus Level 2 & 3 companies to obtain PCI certification is quite significant. As a Level 1 compliant company, I can tell you we made a large seven figure investment in accomplishing the validated certification and implementing ongoing processes!

The required commitment, money and dedication may be a large reason that many companies are either still in the process of meeting the standard or avoiding it altogether. According to data collected by VISA, 65% of Level 1 merchants and 42% of Level 2 merchants are currently PCI compliant even though the deadline for compliance has passed. Yet, failure to meet the standard can be a critical, costly mistake. A recent report from Solidcore Systems estimated that the cost for merchants and service providers not meeting the PCI requirements can be 20 times greater than the cost of proactively becoming compliant.

PCI and Call Center Operations

While the financial and retail industries initially pushed for the tighter security measures, data protection is now a critical issue for companies across the board. The chart below (Source: Identity Theft Center) shows the number of reported breaches by industry.

Sector	Incidents	Affected Records
Retail	24	95,171,110
Services	17	8,901,455
Financial	39	8,793,719
State Government	58	5,948,395
Federal Government/ Military	22	4,017,163
Local/County Government	33	2,381,447
Health Care	56	1,027,462
Technology/Telecommunications	19	899,450
Higher Education	8	680,715
Miscellaneous	54	344,051
Secondary Education	25	85,527

The only way to be assured there are reasonable controls in place is if vendors meet the same standards as the merchants. One non-compliant company within a network can expose the other companies to risk. For this reason, most companies now won't consider working with a vendor, including a call center, that isn't 100% PCI compliant.

The process for call centers to meet PCI standards is time-consuming. It requires extreme attention to detail and the commitment of your entire organization. For brick and mortar centers, it is slightly easier because most of the infrastructure and data is on-premise. Virtual call centers using home-based customer service representatives face additional requirements due to the nature of a dispersed workforce. For example, information must be protected as it travels from the agent through the call center hub to the retailer applications. This involves securing thousands of home-office locations in addition to the corporate headquarters. While it is harder for virtual call centers to become achieve validation of PCI compliance, companies that are well-run and organized with knowledgeable IT personnel can get the job done.

Meeting PCI standards isn't easy. Not only do you need to implement the appropriate measures, but you have to validate to a third party assessor that everything is done correctly. On the other hand, much can be learned by going through the process and your organization will be stronger in the end. Handling sensitive personal information is serious business. The very nature of call centers requires trust from consumers, clients, partners and vendors. As call center executives, we have responsibility to do everything we can to protect this data. These standards provide a roadmap for reducing risk to your systems and will give clients peace of mind knowing you've done everything possible to protect against fraud. Meeting PCI standards is not only critical for the success of your business; it's also the right thing to do.