

## Data Security Standards for Call Centers

by Jim Beuoy, Director of Quality Assurance and Corporate Compliance,  
& Dan Werner, National Sales Director,  
OKS-Ameridial Worldwide

---

Is the industry worried about credit card "PCI" standards? Is a teleservices company a "service agency" for purposes of the PCI rules? The answer is "Yes, they should be." And... "Yes, they are." Payment Card Industry (PCI) Data Security Requirements (articulated in the Consumer Information Security Program) apply to all members, merchants and service providers that store, process or transmit cardholder data.

Granted, the Payment Card Industry may not have direct regulatory authority over call centers, but it is safe to say that if data is compromised while in your center's possession, someone is going to be very unhappy! Technically, credit card companies have a contract with the financial institutions that end up processing / posting credit card charges. Failure to comply with the PCI security standard can result in substantial fines and permanent expulsion from card acceptance programs. Call centers should be concerned because the PCI standards require that the financial institutions hold their down-line support services (i.e., the actual merchant and the other service providers) in compliance with the standards.

...safe to say that if data is compromised while in your center's possession, someone is going to be very unhappy!

There are some other statutes under which call centers are more directly reliable, and we will get to those in a minute. For now, it's best to recognize that failure to apply the PCI standards could end up with serious damage to your brand, your clients' brand, and, ultimately, to your clients' credit card (charges) processor.

Taking credit card orders and posting them directly via your clients' portal, such as their website, doesn't create a great deal of exposure to these standards. However, since the standards make specific reference to service bureaus that store or transmit, call centers that capture credit card information (say on your own screens), store that data, and then later transmit that data to their client, should strongly consider ensuring compliance with the PCI standards.

Requirements include:

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

These stipulations went into effect in June 2005. Unfortunately, they seem to have caught a lot of companies by surprise. In a recent survey at a major marketing association conference, no companies were in compliance with the new standards! Both [www.usa.visa.com](http://www.usa.visa.com) and the corresponding Master Card web site spell these requirements out pretty clearly. On the positive side, most service bureaus and in-house operations are probably 85-90% in compliance. Most companies already have privacy policies put in place, controlled access to their physical facilities, centralized data storage and additional safeguards when accessing data storage. Virtually all companies have reasonably effective firewalls in place and virtually all only allow agents to access essential data elements. Where we seem to come up short (as an industry) is in encryption and intrusion detection software.

Encryption software is cheap. A simple Internet search will yield scores of commercially available options. If you're still emailing data, you're probably putting yourself at risk. It's much safer to post data and recordings to an FTP site that is password and ID protected. In fact, all data needs to be protected by "not commonly known" passwords and ID's that are changed with some reasonable frequency.

Likewise, there are a host of options for intrusion detection software. Approaches to monitoring access to data as well as tracking the "footprints" of what data elements were touched vary from product to product, so your IT Department should look at those options to determine the best course of action for your budget.

In addition to the PCI standards, the FTC has filed against seven companies for insufficient data security protections. Those entities that lose data due to breach are liable for the replacement costs of issuing replacement credit cards. That fee is currently around \$60 per card; however, these costs will pale in comparison to other possible actions.

Arguably, the most publicized enforcement action (regarding data security) by the Federal Trade Commission (FTC) was against Dallas Shoe Warehouse (DSW). The charges can serve as framework to guide you in shoring up your data security initiatives. In this case, the FTC charged that DSW:

- Created unnecessary risks to sensitive information by storing it in multiple files when it no longer had a business need to keep the information
- Failed to use readily available security measures to limit access to its computer networks through wireless access points on the networks
- Stored the information in unencrypted files that could be easily accessed using a commonly known user ID and password
- Failed to sufficiently limit the ability of computers on one, in-store network to connect to computers on other in-store and corporate networks
- Failed to employ sufficient measures to detect unauthorized access

Full details of that action: <http://www.ftc.gov/opa/2005/12/dsw.htm>

DSW has estimated that compliance of the Consent Decree with the FTC will cost between \$6.5 million and \$9.5 million.

If you don't currently have these standards in place, you need to quickly take corrective action on each of the following items:

- Complete inventory of what information is held and where it's held
- Written policy on how employees use data
- Written policy on how we share data (with clients, subcontractors, etc.)
- Written policy on how we protect data
- Password protections (not commonly known, changed with some reasonable frequency)
- Encrypted credit card and social security numbers

- What agents see (only last 4 digits of client provided credit card numbers)
- Log of data purges
- Unauthorized detection safeguards
- Monitored access
- Independent audit
- Plans for notifying consumers whose data has been compromised
- Plans for notifying government when personally identifiable information has been compromised

As of the date of writing this article, no less than 36 states have enacted (new) privacy legislation! States define personal data differently. In some states, it can be as little as name and address only. This is odd since that is frequently public record information. States also differ on *how* and *when* you must notify consumers of a data breach. Some are by mail within X-amount of days, and some are by phone within a couple days. Much like state DNC (Do-Not-Call) rules, there is a myriad of requirements.

#### ■ **Conclusion**

Fines for privacy / data breaches are significant. Damage to your brand could be priceless. If you store data, you need to make sure that you are in compliance with these new regulations that may not have been on your radar. Become familiar with the requirements by researching the state statutes and visiting the FTC website and the web sites of Visa and Master Card. Fortunately, there are companies that can walk you through this process. Some offer very low annual service charges for testing your network for intrusion security (four times a year per PCI standards), and they help you make sense of the PCI Self-Assessment Questionnaire. Your Compliance Officer/Team/IT group need to quickly research the state data privacy statutes and develop a plan to meet those respective requirements. Make this a front burner issue so that we don't see your company on front-page news in a negative light!

#### ■ **About OKS-Ameridial Worldwide**

OKS-Ameridial is an international call center with international program management experience since 1987. With 12 years of experience working together, OKS and Ameridial - now operating as a single company - offer their clients an unparalleled record of providing reliable, cost-effective inbound and outbound outsourcing solutions for a variety of industries. The contact centers are located in the United States, Canada and India with sales offices in the U.S., the UK, Canada, and Germany.

Jim Beuoy may be reached at 330-497-4888 or [jebeuoy@oksameridial.com](mailto:jebeuoy@oksameridial.com). Dan Werner may be reached at 866-671-0778 or [dwerner@oksameridial.com](mailto:dwerner@oksameridial.com).



**American Teleservices Association**

**The American Teleservices Association (ATA) is the ONLY association dedicated *exclusively* to the Teleservices channel!**

The American Teleservices Association ([www.ATAconnect.org](http://www.ATAconnect.org)) represents channel users and suppliers that initiate, facilitate, and generate telephone, internet, and email sales, service, and support. Contact centers offer traditional and interactive services that support the e-commerce revolution, provide specialized customer service for Fortune 500 companies, and generate annual sales of more than \$900 billion.

The ATA represents members on Capitol Hill and in statehouses nationwide, presents domestic and international business networking opportunities, advocates teleservices standards for responsible business practices, provides advanced professional education opportunities, defends the teleservices channel in the public realm, and acts as the channel's information clearinghouse.