



American Teleservices Association

The ONLY association
dedicated *exclusively* to the
Teleservices channel

LEARN IMPROVE
GROW

Whitepapers

"Data Security for Call Centers"

3

by Jim Beuoy & Dan Werner, OKS-Ameridial Worldwide

"Five Most Common Telemarketing Compliance Challenges"

6

by Ken Sponsler, PossibleNOW, Inc.

"Offshore Call Centers Face Compliance Challenges But Also Offer Tremendous Opportunities," A White Paper on Compliance Best Practices and Advice from Experts

8

by Ryan Thurman, Contact Center Compliance (DNC.com)

The opinions and viewpoints expressed in these whitepapers represent those of the author and are not specifically endorsed by the American Teleservices Association. The content of these whitepapers are the sole property of the American Teleservices Association and may not be reproduced or redistributed without its express written consent.

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 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. Dan Werner may be reached at 866-671-0778 or dwerner@oksameridial.com.

Five Most Common Telemarketing Compliance Challenges

by Ken Sponsler, General Manager, Consulting and Audit Services
PossibleNOW, Inc

As the General Manager of PossibleNOW's compliance and audit services division, I have a unique view of industry-wide challenges for telemarketing compliance. Our on-site compliance assessments have included several Fortune 500 sellers as well as numerous service provider operations.

We have found companies struggling with these top five challenges:

- 1. Knowledge of the Rules:** The myriad of state and federal rules and lack of pre-emption is often the number one obstacle of compliance. This is particularly true for companies that have diverse telemarketing programs and conduct multi-state campaigns. Often, compliance with telemarketing regulations is thrust upon the already burdened shoulders of corporate compliance staff. While compliance with SOX, GLB or HIPAA may be within their scope of expertise, telemarketing compliance may not.

If your compliance processes and procedures are not written, trained, monitored and enforced, you do not have a compliance program.

Here are just a few questions your company must be able to answer:

- a. Is our telemarketing activity regulated by the FCC, FTC or both?
- b. If your company has several divisions, how many versions of the National Registry (SAN) are you required to purchase?
- c. Are you registered in states that require sellers (with no in-house, outbound calling) and telemarketers to register as a telemarketer and/or purchase their DNC lists?
- d. Are you complying with the multitude of state EBR rules that are more stringent than federal rules?
- e. Does your company meet the provisions for DNC and Call Abandonment Safe Harbor?
- f. Are agents that are calling on your behalf complying with certain state requirements to disclose your telemarketer registration number upon a sale?

- 2. Possessing Written Compliance Guidelines:** This is one of the most important documents you need should you ever have to respond to a CID. Unfortunately, during a recent compliance assessment for a major corporation that utilized 18 outbound call centers, none could provide a compliance guidelines document.

The foundation of any viable compliance program is the corporate compliance guidelines document, yet few companies have invested the resources to create it. This document describes what rules the company must comply with and how compliance is achieved. It also assigns responsibility and includes training requirements as well as monitoring and enforcement methodology. If your compliance processes and procedures are not written, trained, monitored and enforced, you do not have a compliance program.

- 3. Meeting Recordkeeping Requirements:** This observation stems from experiences in compliance assessments as well as performing forensic data analysis in support of attorneys who are defending clients under investigation. Just as important as having written compliance guidelines is the necessity to have records of compliance. Again, if you cannot prove compliance, you may be found to be out of compliance.

Many campaign related records are required to be maintained for at least 2 years, while DNC records must be maintained for up to 10 years. But maintaining records for your own defense should go well beyond the minimal regulatory requirements. This is particularly important when sellers and call centers share the compliance burden.

If your company is being investigated for alleged violations that occurred two years ago, can you produce records of scrubbing activity, scripts, campaign management, calling records, call abandonment rates, required disclosures, etc? Do you have the compliance records from clients or call centers you no longer do business with?

- 4. Possessing Mutually Supportive Due Diligence:** Some major enforcement actions have highlighted the importance of this requirement. However, we still see far too many companies that lack sufficient due diligence, including monitoring and enforcement processes. Compliance must be mutually supportive. Sellers and call centers must understand the entire scope of the requirements, define which party is responsible for each element and then monitor and enforce compliance.

Sellers must provide compliance documentation to call centers to include event triggers and dates for EBR campaigns. Call centers must ensure DNC requests and DNC policy fulfillment activities are reported back to clients. Sellers should approve scripts before use. Both the seller and the call center should monitor and enforce script content and adherence. The call center should monitor call abandonment rates and report this to the seller on a regular basis.

- 5. Having a Defendable Position:** No one possesses unlimited resources for compliance. But, too often, we see companies that throw their resources at compliance with no overarching plan to achieve a defendable position.

A defendable position means that you possess sufficient written guidelines, compliance processes and monitoring and enforcement procedures to reduce or even eliminate enforcement action liability. These procedures demonstrate due diligence and ongoing efforts in a convincing fashion.

Attaining a defendable position should be the minimal first rung on the ladder to compliance best practices. Companies must determine their compliance gaps and the associated risks. Risk levels can be reasonably determined through an analysis of enforcement history, level of non-compliance and magnitude of the potential fine or public relations damage. A defendable position ensures that the essential compliance processes, procedures, training and record-keeping are in place. A defendable position is inclusive of DNC and Call Abandonment Safe Harbor.

Finally, monitoring and enforcing all of the above challenges rounds out a solid and defendable position program.

■ **About PossibleNow**

From its inception in 2000 to the present, PossibleNOW takes pride in designing, developing and implementing online applications and consulting services that provide our customers with quantifiable value. PossibleNOW provides DNCSolution, a family of Internet-based products that handle the full range of Do Not Contact (Do Not Call, Do Not E-mail, Do Not Mail, Do Not Fax, and Privacy) compliance.

For questions about these challenges or other marketing compliance topics, you may contact Ken Sponsler via e-mail at ksponsler@possiblenow.com.

Offshore Call Centers Face Compliance Challenges But Also Offer Tremendous Opportunities

A White Paper on Compliance Best Practices and Advice from Experts

by Ryan Thurman, Director of Sales & Marketing,

Contact Center Compliance (DNC.com)

With the growth in near shore and offshore call centers over the past few years, the level of concern over adherence to compliance regulations has also increased, especially with a greater level of enforcement and the potential for devastating negative publicity combined with costly fines and legal fees.

The trend towards consumer protection laws on a global scale is clear when you run a quick news search on Google for 'privacy notification laws' or even 'Do Not Call', for example. Canada, Australia, and India are moving forward with do not call regulations modeled after the U.S. Federal Registry. Monitoring and making sure that your offshore or outsourced contact center is adhering to the extensive, tangled web of telemarketing compliance regulations is a challenging task even for U.S. companies, let alone call centers providing near shore outsourced options in the Dominican Republic, Costa Rica, or traditional offshore opportunities in the Philippines or India. Combine these factors with other comprehensive rules surrounding predictive dialer abandonment rates, wireless compliance, non-rebuttal states, non-profit calling campaigns outsourced to a for-profit call center operation. Plus, add in the privacy regulations surrounding required notifications for breach of personal identifiable information, and you start to realize that there are innumerable ways Federal or State officials can get their nose under the tent and wreak havoc on your call center operation.

Fortunately, the good news is that the total percentage of call centers that are in compliance is very respectable

■ Most U.S. Firms are Ahead of the Compliance Curve

Fortunately, the good news is that the total percentage of call centers that are in compliance is very respectable when you look at the adherence to the Federal Do Not Call program in the U.S. compared to all of the millions of calls telemarketers make annually in the U.S. There is a relatively small amount of calls to phone numbers on the Federal Registry; however, many offshore centers have realized that enforcing laws in other counties may be a long, drawn-out process, such as in India, where it may take up to seven years to even bring a case to trial. There is benefit that has come from compliance regulations. For call centers that outsource work to offshore firms, the sellers are increasingly requiring concrete documentation, site inspections, surprise audits and synchronized and approved compliance technology to verify that they will not end up on the front page of the business section. There is a good deal of effort for the outsourcer to demonstrate compliance because it leads to long-term business sustainability and can be used as a value-added selling point in the very competitive, billion dollar outsourcing marketplace.

The North American call center outsourcing market is expected to continue along a steady growth path, according to recent research by Frost & Sullivan Inc., which states that the market reached \$19.5 billion in revenues in 2005 and is expected to reach \$20.1 billion by 2012. Call center agent attrition, companies continuing to adjust to Do Not Call legislation and greater specialization by North American outsourcers are driving the market, according to Michael DeSalles, Frost & Sullivan's industry analyst for the communications practice.

The trend toward outsourcing will inevitably continue due to the significant return on investment by having access to a larger labor pool with lower wage requirements than in the U.S. This savings can translate from 50-70 percent less than onshore facilities with a labor pool that often has a higher

education and experiences a lower turnover rate. The return on investment benefit brought about by your new offshore call center can be offset negatively by just one of your outside vendors that fails to comply with any of the Federal or State compliance rules. While the fines can range in the millions of dollars, as with Direct TV, the actual cost of compliance is much less than that for most organizations, hence the need to understand where you can push for best practices in your call center and with offshore partners.

■ **Compliance Best Practices Can Avert a Train Wreck**

While compliance is usually an increasing annual budgeted expense for most companies in the U.S., offshore centers oftentimes have a different take on implementing best practices. One benefit clients have witnessed with the Federal Do Not Call Registry is that response rates for some verticals of consumer goods have gone up since the Registry has grown in size to over 132 million numbers. Offshore centers in many markets have seen this as well, and it has spurred many to increase their focus on compliance. However, some countries and offshore locations provide a haven for the bad apples in the call center business to proliferate. Just take a look at Canada, where it was recently estimated by the FTC that Canadian call centers are responsible for approximately \$100 million in illegal business annually, thereby harming U.S. consumers. In comparison, InternationalStaff.net estimates that South Asian call centers operating illegally are currently generating four to five times that amount in total revenue. In addition, InternationalStaff.net estimates that in India, on any given business day, there are at least 300 call centers actively engaged in violations of U.S. telemarketing rules and that the actual number of outlaw facilities in India could be twice that figure if unincorporated operations and those with less than 10 seats are included. According to Workforce Management's Matthew Heller, Consecro, Inc. sold its India-based ExlServices because customers complained that they could not understand the call center agents, and Dell Computers pulled two of its products out of an Indian call center due to similar customer complaints.

E-commerce Times' columnist, Anthony Mitchell, estimates that less than 12 percent of Indian call centers comply with state telemarketing rules. Mitchell has worked with the Indian IT industry for 17 years, and he specializes in offshore process migration and call center program management. "Even though your own firm's programs may be in compliance," Mitchell asserts, "having out-of-compliance programs running in tandem at the same offshore facility presents risks of collateral damage in the event that enforcement efforts ever target that facility operator."

Since the advent of Voice Over IP (VoIP), call centers are sprouting up all over areas that now have enhanced telecommunications access. This has led to an increase in credit card scams, automated dialers that are used with pre-recorded messages, and other major compliance issues due to the lack of international enforcement. The FTC and State Attorney Generals in the U.S. have thus far pursued several well-known U.S. corporations that violated compliance rules and even U.S.-based outsourcers. There has been little news about offshore enforcement.

■ **Implementing Compliance Offshore: Do your Homework**

One of the benefits of outsourcing offshore lies in the educational background of many local economies where a job in a call center is considered a prominent position. In the call center business, your lowest paid employee is your main defense to ongoing daily compliance such as scripting rules or in-house do-not-call or policy requests. With a better-educated work force and more dedication to the call center as a career, more concern about compliance and following the rules goes hand-in-hand. This is one reason certain markets like the Philippines, Panama and Costa Rica are exploding as sellers are becoming increasingly confident in these countries' abilities to deliver results and document compliance across the enterprise.

Starting a relationship with an offshore center is akin to getting a prenuptial agreement in the global marketplace—you want to put controls in place so that you don't get burned! As a seller, you may

want to control things like making sure the data stays in your possession or the calls are routed through your U.S. switch so that you can monitor quality and compliance. You also may need to support the outsourcer with clarifications on so-called "legal gray areas" so that everything is black and white in the agreement.

Proper due diligence and reference checks will help you uncover any previous issues. Ensure that the firm has a dedicated compliance officer and that they have all the necessary policies in place, as well as any necessary State registration and bonding requirements up-to-date. Clarify the use of the client's Federal Registration (SAN number) and if calls will be placed under any Existing Business Relationships (EBR's) or under any industry exemptions such as non-profit, supervised financial lender or newspaper/magazine seller. Make sure there are no deviations from scripts and that proper scripts are populated to account for non-rebuttal states. Newer technologies such as NICE Systems allow you to pinpoint deviations from scripts or key phrases such as "Put me on your do not call list" so that remote monitoring is not only effective for quality, but also for compliance escalation processes where database centralization is critical.

■ **Technology Solutions Enable Business Enabling Best Practices**

As we have seen with the majority of the enforcement actions to date, the number one impetus for a State or Federal investigation is the result of do-not-call violations. This is, in part, because the average U.S. consumer does not realize there are exemptions to the DNC list and that being on the list will not stop all telephone solicitations. They may not be aware because they are an existing customer or may have, for example, visited a vacation property that employs telemarketing calls. Hence, the importance of mitigating potential complaints before they are escalated to a regulatory authority and the importance of working with your outsourcer to have a compliance escalation plan.

For companies that outsource their call center work offshore, there is certainly more complexity when trying to stay updated with current DNC laws and the multiple DNC lists, while also adhering to reporting requirements for database centralization across the enterprise. The most efficient way for an enterprise to ensure compliance is to employ the necessary solutions to monitor internal and external processes. The proper solution not only provides the necessary tools to adhere to the Do Not Call regulations, but it can also provide real-time service to keep the call center up-to-date on consistently changing rules.

Compliance technology solutions from a company such as Contact Center Compliance (DNC.com) offer complete automation to save time and expense, the ability to clean lists before calling to prevent violations as calls are being dialed, provide centralized failsafe compliance as well as integrated rules and detailed reporting. DNC.com provides a hosted, rule-based model with an integrated legal matrix that a company with internal call centers abroad or a company outsourcing work overseas can utilize to ensure their data is managed to remove all necessary State and Federal Do Not Call numbers, as well as wireless numbers, by applying the most conservative rules, including Existing Business Relationship (EBR) regulations before calls are placed that automatically centralize the company's calling lists with any new, updated company-specific DNC numbers.

■ **About Contact Center Compliance (DNC.com)**

Contact Center Compliance reduces the complexity of Federal and State telemarketing laws concerning Do Not Call, wireless, and exemptions-including Existing Business Relationships- with an award winning enterprise level technology solution. As the leading full service compliance technology provider for leading call centers worldwide, we manage the entire compliance process seamlessly from the point of first contact through the entire customer relationship. Visit DNC.com for more information.

Ryan can be reached via email at ryan@dnc.com or at 866-362-5478 ext. 116



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) 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.



American Teleservices Association

3815 River Crossing Parkway, Suite 20, Indianapolis, IN 46240 ■ (317) 816-9336 ■ www.ATAconnect.org

