



Compliance with SOX and DNC Regulations is Interdependent when Telemarketing is a Core Part of a Sales Strategy by Lisette Ruch, CPA

Executive Summary

- Compliance with management's internal control assessment provisions of SOX is now a requirement. Time is up!
- Companies are now embracing a more holistic mindset to risk management out of genuine need as demonstrated by the high profile failures to adequately manage risk and the massive financial impact it has had, leading to issues with financial reporting. No longer can risk mitigation efforts be focused solely on compliance, although this is the stepping stone.
- Companies who rely on telemarketing as a key part of their sales and marketing processes face a special challenge, requiring them to embrace a more holistic approach to risk management from the onset. In their world, failure to comply with the Do Not Call (DNC) rules could also lead to failure to comply with SOX since penalties and fines for violations could easily be material to a company's financial information.
- Telemarketers who do not have internal controls in place to ensure that they do not call phone numbers on the DNC lists, could be racking up fines and penalties they don't even know about. And if they don't know about them, they certainly aren't recording them in the financial information. The risk of unrecorded liabilities associated with DNC violations goes unmitigated and most probably unidentified. Furthermore, if a company does not have some kind of DNC solution in place it cannot even reasonably estimate its liability associated with those violations. So there is no effective method of recording liabilities or losses in accordance with applicable accounting rules.
- It is not enough to merely have a DNC solution in place. This solution must be designed properly, having controls within the process or application to mitigate the risks of lack of necessary functionality, circumvention, security, failure, and insufficient monitoring.
- Keeping with the nature of proper risk mitigation, the DNC solution must also be cost-effective, which is a key concern for management. Providers have stepped in to fill the gap and provide effective technology at an affordable price. Management can no longer complain that a sufficiently cost-effective solution is not available.

- Management needs to be aware that its DNC-compliance must be a key part of its SOX strategy and implement or maintain internal controls to address this financial reporting issue and include them as part of its SOX assessment process.

Since enacted in 2002, the Sarbanes Oxley Act has had the management teams of publicly-traded companies scrambling to comply with its demanding hurdles. Having holes in your SOX has meant more than cold feet. While non-accelerated filers have caught a break, the SEC postponed their external SOX-compliance audit for at least one fiscal year and most likely another, this does not exempt management from being SOX-compliant now.

While non-accelerated filers are just achieving or still in the process of achieving this compliance, accelerated filers are beginning to experiment with the “beyond compliance” experience. SOX has generated positive improvements. It has highlighted the need for both management and employees to focus on internal controls and acted as a spring board for management to move from merely mitigating compliance risk to full enterprise risk management. Risk is being looked at from a more comprehensive perspective. The 21st century has already been marked by the need to move from this compliance-based mindset to a more holistic approach, especially in light of the embarrassing failures of high-profile executive teams across many different business sectors to adequately mitigate risk, landing these companies in financial straits and public relations nightmares. In fact, by widening the box, management has come to recognize that many other risks have impacts on their financial reporting and they are transforming the infrastructure they have set up to address SOX to tackle these other risks.

So what does it mean to be SOX-compliant, that first step toward creating a comprehensive risk management strategy? Management must be able to assert that they have analyzed, documented, and assessed the key internal controls over financial reporting using a risk-based approach to focus its efforts on those critical areas of the business. This is no small task considering that management must also include in its assessment the risk of not knowing about or ignoring financially significant transactions, especially unrecorded liabilities.

Companies, both public and private, who rely on telemarketing as a key part of their sales and marketing processes, face a special challenge which is requiring them to embrace a more holistic approach to risk management from the onset. In their world, failure to comply with the Do Not Call (DNC) rules could also lead to failure to comply with SOX. DNC difficulties are massive since both state and federal governments have their own lists. 43 states have their own DNC legislation and the Federal Registry currently has more than 140 million numbers. The chances of dialing one of those numbers without a comprehensive solution are certainly too high. Telemarketers who do not have internal controls in place to ensure that they do not call phone numbers on the DNC lists, could be racking up fines and penalties they don't even know about. And if they don't know about them, they certainly aren't recording and disclosing them in the financial information. The risk of unrecorded liabilities associated with DNC violations goes unmitigated and most probably unidentified. Furthermore, if a company does not have some kind of DNC solution in place it cannot even reasonably estimate its liability associated with those violations. So there is no effective method of recording liabilities or losses in accordance with applicable accounting rules.

The risk of DNC violations is not insignificant. With fines of up to \$25,000 per violation, the unrecorded liabilities associated with them could quickly result in a material misstatement to financial information, and thus, point to a material weakness in internal controls. While settlement amounts agreed to years after investigations have been completed may be much less than the actual fines levied against violators, companies must consider the costs of defending against and appealing these fines over the years while being conservative in estimating and recording liabilities in their financial information. These costs are not taken into consideration in the total settlements reported by the FTC, FCC and state agencies, but must be accounted for by violators. Take for example the \$2.2 million settlement imposed on ADT Security Services and those on its distributors or the \$4.4 million settlement agreed to by Craftmatic Industries, Inc. One company called more than 900,000 numbers on the DNC registries, at \$11,000 per violation, the initial fines are exorbitant and trying to reasonably estimate the amounts to record or disclose as part of financial information is daunting. Many more violations and in-process cases can be found at <http://www.ftc.gov/bcp/edu/microsites/donotcall/cases.html>. Moreover, consumers continue to have the ability to bring a civil action against the violating company and potentially recover civil penalties inclusive of court costs, attorney fees and monetary fines, compounding the issue of unrecorded liabilities.

CFOs of companies who use telemarketing as a strategy not only need to address the financial losses associated with fines but the lack of controls in place to identify these losses. There are some DNC-compliance solutions on the market and some large companies have developed their own in-house processes. The adequacy of a DNC-compliance solution as an effective internal control is dependent on the design of that solution, or, you can think about it as the controls that make up that solution. The solution needs to address the risks of lack of necessary functionality, circumvention, security, failure, and insufficient monitoring. In order to do so, the DNC solution should address the following control objectives in order to maximize the potential for both DNC and SOX risk mitigation:

Functionality Control Objectives

- Real-time, automatic blocking of dialed numbers by all members of the sales organization
- Cross-referencing of dialed numbers against multiple database lists (federal, state, wireless, proprietary/in-house, and override/existing relationship) at once.
- Easy searching feature so that the status of numbers can be looked up individually
- Full add, delete and modify capabilities of your company's or your clients' proprietary in-house lists
- Automatic updates of available federal, state, and wireless DNC lists in accordance with update mandates
- Quick updates to the database to ensure that the operation is using the most recent information.
- Customizable CallerID and CallerName features to manage the number and information that is displayed to individual customers in accordance with the various DNC regulations.

Circumvention Control Objectives

- Policies and training in place to ensure that all users and callers know the proper protocol for initiating telemarketing calls
- Ability to include enterprise-wide locations (even home-based or international) in the DNC solution network
- Functionality for all outgoing calls regardless of how they are initiated (i.e. predictive dialers and other computer-generated calling applications).
- Inability to circumvent the solution (not logging in, dialing special codes, etc.)

Security Control Objectives

- Reliable transmission that ensures that all calls are routed through the appropriate channel to be vetted against your database and not someone else's.
- Encryption capabilities to ensure that data cannot be read if intercepted during the transmission
- Firewall or other intermediary device that properly secures outgoing communications ports to avoid intrusion into the company's IT systems.
- Secure access to the database to ensure that no one has access to the data in the database besides those you have authorized.
- Ability to set security and access levels for all users and administrators
- Multi-factor identification (user name and password) required to access user and administrative features of the solution
- Ability to limit access to overriding the blocking of numbers
- Date stamping and version control (including user information) of all changes to DNC lists and other maintenance features

Failure Control Objectives

- Restriction messages or some obvious notification that call blocking is occurring
- If failure of the solution occurs, inaccessibility to make telemarketing calls so that no violations can occur during that down-time.
- Monitoring of software and hardware used as part of the solution to ensure that solution is operational at all times, including redundancy in case of failure by a component.
- Continuous monitoring and renewing of subscriptions to state and federal DNC lists, which is a pre-requisite of any solution since the data must be collected and current

Monitoring Control Objectives

- Customizable reporting tools to generate reports detailing call by call information, blocking information, and summary information so that the functionality of the system can be monitored.
- Members of management outside of the telemarketing, sales, and marketing departments who are responsible for reviewing reports and handling DNC issues, creating effective segregation of duties.
- Effective record keeping that allows for proof that violation calls were blocked and that business relationships exist with customers who are listed in the registry.
- Demonstration that the solution is in place, being used, and effective

General Controls

- Adequate training of administrator(s) and users to ensure that they are configuring the features of the solution appropriately and using them to their maximum capability
- Testing of the solution before implementation, post-implementation and routinely (at least quarterly) while in production to ensure it is operating effectively and as designed
- Support by knowledgeable and experience communications professionals who can troubleshoot the system and ensure its continued functionality

Management must identify a solution which addresses all of these objectives, but in keeping with the nature of proper risk mitigation, the DNC solution must also be cost-effective. This has been and will continue to be a key concern for management. Providers have stepped in to fill the gap and provide effective technology, which addresses the objectives discussed above to varying degrees, at an affordable price - less than a penny per call. For example, an analysis of Teleblock®, a solution designed by Call Compliance, Inc., has concluded that it meets the vast majority of these control objectives seamlessly. With such a solution, management only has to focus on those considerations related to how access to the solution is granted and developing and enforcing monitoring controls. Steve Carter, the Attorney General for the State of Indiana, submitted comments to the Federal Communications Commission regarding DNC laws in the United States. He stated that “with services such as Teleblock® that provide automatic blocking of restricted numbers, companies should no longer have to monitor each state’s laws, their own campaigns, or the actions of their vendors because the service already does that for them at very little cost. Teleblock® has yet to see one of its customers fined.” Thus, Teleblock® appears to serve as an effective internal control to ensure against DNC violations, so that the risk of unrecorded liabilities is sufficiently mitigated. Thus, having an adequate DNC solution in place not only becomes an effective control to support financial reporting and substantially reduce the risk of DNC violation losses, but a reasonable cost of doing business. Management can no longer complain that a sufficiently cost-effective solution is not available.

Management needs to be aware that its DNC-compliance must be a key part of its SOX strategy and implement or maintain internal controls to address this financial reporting issue and include them as part of its SOX assessment process.

Lisette Ruch, CPA is the President of Sesen Business Regeneration, Inc. (SBR), a risk management consulting firm that has designed and implemented countless SOX compliance projects from inception to audit success across various industries and acted as an advocate for management during their assessment efforts. SBR specializes in helping companies, banks, not-for-profits, and governments perform enterprise-wide risk assessments and strategic and operational evaluations, execute business process analysis and measurement, design and assess internal controls, and develop and implement effective risk management functions, including enlightened internal audit and fraud prevention/detection solutions. SBR also works with entrepreneurial, start-up ventures to build effective business processes from inception and address operational issues specifically tied to development-stage companies. SBR is a 21st century consulting firm built on the idea of comprehensive but cost effective solutions for clients and flexibility, independence, and creativity for its employees. Lisette can be contacted at 727-744-8786 lissetteruch@aol.com.