



Critical Call Recording Laws, Regulations and Best Practices for Ensuring Compliance

Authored by
Dick Bucci
Associate Consultant, The PELORUS Group



Sponsored by





Table of Contents

Goals and Scope of this Guide 2

Payment Card Industry Data Security Standard (PCC-DSS)..... 3

Telemarketing Sales Rule (TSR) 4

Truth in Lending Act (TILA)..... 6

Fair Debt Collections Practices Act (FDCPA) 7

Consent to Record..... 8

Health Insurance Portability and Accountability Act (HIPAA)..... 9

Family Medical Leave Act (FMLA) 10

To Learn More 11

Summary 12

About the Author..... 13

About VPI 13

Running a contact center requires more skill sets than just about any other position in the enterprise. Managers are expected to be information technology experts, finance whizzes, inspirational coaches, and occasionally amateur psychologists. Dare we add lawyers? Not necessarily, but compliance is playing a larger role in contact center performance than ever before. Violations can be very costly - not just in financial terms but in customer credibility as well. This does not mean you need to take time off to attend law school, but it does mean that you need to at least be aware of some of the many laws, regulations, and industry standards that most profoundly effect contact centers. You also need to know what you can do to avoid problems and where to go when you need help. Fortunately, many progressive vendors have incorporated features in their applications that help you comply.

Goals and Scope of this Guide

First, reading this paper won't make you an expert and won't relieve you of the necessity of checking with your compliance officers or legal resources in time of need. However, we can almost guarantee that you will learn something new and have a better understanding of the current legal and regulatory environment as it concerns your specific responsibilities. ***We can't emphasize enough that this is a very handy resource guide, not a legal document.*** We recommend that you become a member of a trade association that retains legal counsel and issues periodic alerts and guidelines. If your firm or organization has a compliance office, work closely with them to assure that the steps you take are the correct ones and in keeping with overall corporate policies and IT established processes. For more details, please refer to the table of resources on page 11.

There are literally hundreds of federal, state, and local regulations that can affect contact center practices. We will discuss only the statutes and standards that - in the author's view - most directly impact contact centers. Further, the scope is limited to the United States, and primarily federal - not state - laws and regulations. Federal laws apply to interstate commerce. Typically, individual states enact similar legislation to address intra-state commerce. It is not unusual for state laws to be more restrictive than federal laws.

The following table lists the statutes and standards covered in this paper and their primary focus.

	Abrev.	Fraud	Abuse	Privacy	Labor
Payment Card Industry Data Security Standard	PCI-DSS	•		•	
Telemarketing Sales Rule	TSR	•	•	•	
Truth in Lending Act	TILA	•		•	
Fair Debt Collections Practices Act	FDCPA	•	•	•	
Consent to Record	CTR			•	
Health Insurance Portability and Accountability Act	HIPAA			•	
Family Medical Leave Act	FMLA				•

Payment Card Industry Data Security Standard (PCC-DSS)

Credit card fraud is a growing menace. According to the US Department of Homeland Security, the cost of credit and charge card fraud may be as high as \$500 million a year. Identity theft was the number one source of consumer complaints to the FTC in 2007. And it's not just the credit card companies that are left holding the bag - cardholders often face economic losses, lengthy legal battles and struggles to re-establish clean credit records.

In order to reduce fraud, the Payment Card Industry (PCI), which consists of American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, established the PCI Security Standards Council in September 2006. The aim of the council was to establish a set of rules that merchants and service providers must comply with in order to accept payments through the credit and debit card apparatus set up by the card vendors. While the council is managed by the card industry, membership is open to any organization that participates in the payment processing system, including: merchants, processors, POS vendors, and financial institutions.

The council subsequently issued a Data Security Standard (PCI-DSS) which details security requirements for members, merchants and service providers that store, process or transmit cardholder data. The PCI regulations specifically forbid storing unencrypted credit card numbers, PIN numbers, and other specified identifiers. Payment processors, service providers and merchants that process more than 20,000 e-commerce transactions and over 1 million regular transactions are required to engage a PCI-approved Qualified Security Assessor (QSA) to conduct a review of their information security procedures and scan their Internet points of presence on a regular basis. However, no organization that accepts cards issued by the founding members of the council is exempt from compliance.

PCI-DSS is not a federal regulatory requirement. Merchants and service providers that do not comply are subject to breach of their contracts which can result in termination of card acceptance privileges and subsequent business losses. Minnesota and Texas have codified the PCI-DSS and at least 22 other states have enacted data security laws of some types. Others are in the process of formulating legislation.

While the standard is primarily aimed at cardholder information in data bases, contact centers can easily become unsuspecting violators. This is because of the practice of collecting and entering card data into order entry systems and recording private customer information in call and data recording systems. Unless agents are specifically authorized to see this information, their unrestricted access is a violation of PCI-DSS and an unnecessary risk exposure. You can avoid potential violations by assuring that your CRM or order processing system masks and mutes card information and by investing in recording technology that blocks or encrypts recordings that contain card numbers. Your recording software should be able to encrypt, mask, or mute card data from voice recordings and archived computer screen recordings.

Best Practice Tips

- ✓ *Work with your information technology department before implementing contact center-specific solutions. Compliance is an organization-wide commitment. IT may have an overall security plan that contact centers must adopt. For example, individuals that require access to archived calls that may include card data must be specifically authorized to access this information.*
- ✓ *Make sure your order entry, new customer applications, and any other customer data bases that your agents frequently access mask out credit, debit, and other sensitive information.*
- ✓ *Find out how your current recording software handles PCI-DSS compliance. Some vendors do not have a solution. Others may require deleting entire interactions that involve card transactions, making it impossible to conduct quality evaluations on these calls or retrieve them for compliance or verification purposes.*
- ✓ *If you are considering a new interaction recording system, look into the approach adopted by VPI. VPI provides secure, end-to-end encryption at no extra cost. For companies that prefer a more flexible approach, VPI CAPTURE call recording software can automatically detect when an agent enters a screen where a credit card field is to be filled out and then mask both the voice and screen entries for the duration of the agent's activities while working in those screens. The recorder then reverts to normal recording mode. Voice and data recordings mask the sensitive information, which can only be accessed by authorized personnel.*
- ✓ *Make sure you maintain strict processes that prevent agents from jotting down card numbers for later entry into the customer data base.*

Telemarketing Sales Rule (TSR)

The Telemarketing Sales Rule is the most comprehensive federal legislation aimed directly at contact centers. While the primary intent is to prohibit fraud and abuse in outbound telesales environments, the TSR also applies to inbound and blended environments if they engage in up-selling. Some organizations are exempt, such as political campaigns, charitable organizations, third party fundraising firms, common carriers, and certain financial institutions. Certain types of inbound calls are also exempt, such as unsolicited hotel reservations.

The TSR requires material disclosures before orders may be accepted by phone. The specific disclosures are spelled out in the TSR, but in general they include disclosing the identity of the seller, the nature of the goods or services offered for sale, the full cost of all offers, any conditions or restrictions associated with the offers, and business policies - such as handling order cancellations and returns. The disclosures may be made by mail (in advance of accepting the order) or by phone during the telemarketing call. There are special rules for up-selling. If the second transaction in a single call involved a second seller, then the identity of the second seller must be provided. Another important provision prohibits sellers and telemarketers from making false or misleading statements. The FCC may assess a fine of up to \$11,000 per violation.

Depending on the method of payment, the seller may be required to obtain “Express Verifiable Authorization” (EVA) from the buyer. EVA may be secured in one of three ways: advance written authorization from the consumer, written confirmation from the seller before the transaction is submitted for payment, or an audio recording in the customer’s voice confirming the order. For added security, telemarketers will often transfer the call to a supervisor or other individual who will ensure that all disclosures were made and will ask for the customer’s concurrence. Of the available verification methods, call recording is the fastest, most convenient, and most foolproof. The audio recording must demonstrate that the buyer was provided with seven specific pieces of information.

The Do Not Call provisions prohibit telemarketers and sellers (excluding exempted callers) from calling phone numbers that are on the Do Not Call Registry. Agents may initiate outbound calls to individuals with whom they have an existing relationship. This provision extends to third party collection agencies.

There are now more than 155 million telephone numbers on the Registry. Since the FCC began enforcing compliance with the Registry in 2003, the agency has secured more than \$16 million in civil penalties and more than \$8 million in consumer redress.

There is a common misconception that the TSR applies only to big telemarketing organizations. Not true. The rule applies to telephone sales workers, telemarketers, telefundraisers, and sellers. There are no business size limitations.

Best Practice Tips

- ✓ *Create scripts that assure that all required disclosures are made by the agent.*
- ✓ *Train agents on TSR requirements that directly effect the way they do their jobs.*
- ✓ *Record all voice and screen interactions that involve actual telephone sales or sales attempts.*
- ✓ *For maximum speed and convenience for retrieving calls pertinent to specific sales or sales attempts, consider investing in speech or screen analytics software. This is very helpful for dispute resolution.*
- ✓ *Telemarketing organizations should ensure that the latest Do Not Call registry is loaded on their dialer software and that the software can automatically detect and block calls to individuals on the list.*
- ✓ *Dialers should also be programmed to permit calls only during the times during which calls can be made (8:00 am to 9:00 PM)*
- ✓ *Pre-recorded sales messages are prohibited.*
- ✓ *Your organization must be adequately staffed to take live calls within two seconds of the time a person answers the call and the automated greeting is completed. A safe harbor provision exempts organizations that use a dialer that ensures no more than 3% abandonment of answered calls.*

Truth in Lending Act (TILA)

The Truth in Lending Act is intended to help assure that consumers are made fully aware of terms and conditions related to consumer loans. The Act also gives consumers the right to cancel certain credit transactions that involve a lien on a consumer's principal dwelling, regulates certain credit card practices, and provides a means for fair and timely resolution of credit billing disputes. Disclosure rules are addressed in Regulation Z. Subsequent amendments prohibit the unsolicited distribution of credit cards and tighten disclosure requirements for home equity loans. TILA is primarily directed towards consumer lending institutions including banks, credit unions, and finance companies.

TILA differentiates between closed-end financing and open-end accounts. Closed-end lending refers to loans with a definite term, such as auto loans and home mortgages. Open-end credit refers primarily to credit cards, home equity lines of credit, and other instruments that do not have fixed installment schedules. TILA does not apply to commercial loans, loans to government instrumentalities, credit in excess of \$25,000 not secured by real property, student loans, and securities brokers.

Contact centers that are involved in home mortgages, credit cards, and other consumer lending activities must be aware of the material disclosures required by TILA. Disclosures are typically provided in writing prior to consumer acceptance of any loan agreement but may also be provided during telephone interactions. The growing trend to marketing credit cards and other loans over the Internet has increased pressure on contact centers to understand the disclosure requirements of TILA. Applicants that are having trouble navigating the web site will call the toll-free number for assistance.

TILA provides very specific disclosure requirements for lenders. Examples include the methods by which interest rates are calculated, requirements to disclose the annual percentage rate, cost of late fees, payment term, advance notice of renewals and many other items consumers should know when evaluating the cost and terms of credit.

Best Practice Tips

- ✓ *Record all voice and screen interactions. Increase evaluation frequency for new agents - check voice and screen recordings for disclosures and accuracy of data entry. Consider adding screen analytics applications that automatically tag and categorize recordings based on events that occurred during the call. This will help you quickly locate recordings that require frequent review.*
- ✓ *Prepare training materials and scripts that help assure that all mandatory disclosures are made.*
- ✓ *Update these materials every time there is a change in interest rates or payment terms.*
- ✓ *Provide agents with a list of subject matter experts in the event they need further clarification*
- ✓ *Review procedures with your compliance office*

Fair Debt Collections Practices Act (FDCPA)

The FDCPA is designed to eliminate abusive, deceptive, and unfair debt collection practices. It also protects reputable debt collectors from unfair competition and encourages consistent state action to protect consumers from abuses in debt collection practices. While the FDCPA generally applies only to third party collectors, some states such as California have state consumer protection laws which mirror the FDCPA, and regulate original creditors as well. Both third-party and in-house collectors must also be familiar with state bankruptcy and consumer protection laws. The largest violation to date was against debt collector *LTD Financial Services*, which agreed to pay \$1.3 million in civil penalties to resolve charges that it misled, threatened, and harassed consumers.

The FDCPA mandates when calls can be placed (between 8:00 am and 9:00 pm), who can be contacted (only the debtor or his/her attorney), and where calls can be placed. When calling debtors, collectors must identify themselves, including the name of their firm, and explain that the purpose of the call is to collect a debt (“Mini-Miranda”). Among other provisions, the law expressly prohibits false, deceptive, or misleading representation or means in connection with the collection of any debt.

Third party collection agencies are a major source of complaints to the Federal Trade Commission. Agencies that want to keep their clients and prosper in this highly competitive narrow-margin business must be on their toes to assure compliance. Since collectors have an existing business relationship with debtors, they are not subject to the TSR.

Best Practice Tips

- ✓ *Agencies can't do too much training. The latest eLearning and eCoaching applications help you maximize the impact of your training while controlling costs by employing a very efficient training methodology - these applications deliver training content at the right time and in the right context, targeted at needs and skill gaps of each and every agent individually.*
- ✓ *All interactions should be recorded and archived for compliance and liability protection.*
- ✓ *Collectors should have scripts that assure that essential disclosures are made and evaluation procedures should monitor adherence to these scripts.*
- ✓ *If they accept payment by credit or debit card, agencies are also subject to PCI compliance. This can pose a problem if their recording software permanently masks or deletes entire interactions that involve such payments.*
- ✓ *Advanced solutions such as the one offered by VPI allows the agency to either encrypt the entire interaction or mask only the voice and data interactions that occur when the agent enters specific customer data collection screens in the collections software.*
- ✓ *Dialer software should be programmed to prohibit calls during excluded hours and block calls to debtors who have formally requested that calls be stopped.*

Consent to Record

The Federal Electronic Protection Act (ECPA) permits recording telephone calls and in-person conversations with the consent of at least one of the parties. Thirty-eight states and the District of Columbia have adopted one-party consent laws. The other twelve states generally require the consent of at least two parties to the call. These states are:

- | | |
|------------------------|------------------------|
| ✓ <i>California</i> | ✓ <i>Nevada</i> |
| ✓ <i>Connecticut</i> | ✓ <i>New Hampshire</i> |
| ✓ <i>Delaware</i> | ✓ <i>Pennsylvania</i> |
| ✓ <i>Florida</i> | ✓ <i>Vermont</i> |
| ✓ <i>Maryland</i> | ✓ <i>Washington</i> |
| ✓ <i>Massachusetts</i> | ✓ <i>Illinois</i> |

In Connecticut, consent must be obtained either in writing or orally at the beginning of the recorded conversation. So, which laws take precedence, state or federal? In a California court case (*Kearney v. Salomon Smith Barney*), Georgia-based stockbrokers recorded calls to and from California customers. The brokers did not advise their customers they were being recorded and argued before the court that notice was not necessary because Georgia is a one-party consent state. The court held that the California law - which requires all party consent, should govern.

So what constitutes “consent”? The courts have ruled that providing advance notice that the call will be recorded is sufficient. Consent is implied if the called (or calling) party continues the conversation after hearing the verbal warning. In all-party consent states employees must also consent to being recorded or monitored.

Similarly, the called or calling party may record the agent - provided legal notice is provided. Another possibility is that the calling or called party may request a copy of the recording. They have the right to ask, although unless subpoenaed, contact centers are not required to provide the recording.

Best Practice Tips

- ✓ *If you are recording calls and communicate with customers or prospects in multiple states, always precede the call with a notice that the call may be recorded.*
- ✓ *If you operate in only one state and that state requires only one-party consent, then the notification is not necessary. However, it is still good customer relations practice to provide the advance notification.*
- ✓ *It is always good practice to advise agents via employee handbooks or even signed agreements that they may be recorded for training and quality control purposes.*

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was enacted in 1996 to promote the continuity and portability of health insurance, fight fraud and abuse, establish medical savings accounts, and other purposes. The law distinguishes between “covered entities” and “business associates.”

CE - Covered Entity

CEs are basically any person, business, or government entity that furnishes, bills, or receives payment for health care in the normal course of business. Examples include physicians, hospitals, pharmacies, health care clearinghouses and health insurers.

BA - Business Associate

A business associate is a person or organization that performs a function on behalf of a covered entity. Examples include software vendors, third party billing companies, claims processors, collections agencies, and outsourced contact centers. BAs must also agree to the privacy and data security requirements of HIPAA.

A business associate could be a contact center outsourcer that handles calls for a covered entity or a collection agency working on their behalf.

The **Privacy Rule** is a key provision of HIPAA that most directly effects collection agencies and contact centers. Among other things, the Privacy Rule requires:

- ✓ Notifying patients about their privacy rights and how their information can be used.
- ✓ Adopting and implementing privacy procedures
- ✓ Training employees so that they understand the privacy procedures.
- ✓ Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them and are not authorized to view them.

The privacy rule protects all “individually identifiable health information” held or transmitted by a covered entity or its business associate, whether electronic, paper, or oral. The Privacy Rule calls this “protected health information (PHI).” This is a very broad definition that encompasses just about any information that relates health information to specific individuals. Examples include common identifiers like name, address, birth data and social security number. There are a number of exceptions where release of PHI is permissible and two instances when PHI must be disclosed. A covered entity may secure the patient’s written authorization to release PHI. A central tenant of the Privacy Rule is the principle of “minimum necessary” use and disclosure of PHI.

The fundamental implication for covered entities and their business associates is that PHI must be protected.

Best Practice Tips

- ✓ *In house call centers for covered entities (e.g., providers, insurers, etc.) and business associates (collectors, outsourcers, billing companies, etc.) should have strict controls over customer data bases. Non-authorized personnel should not have access to information about the health condition of specific individuals.*
- ✓ *Covered entities must have specific policies and procedures that restrict access to PHI.*
- ✓ *If the covered entity or third-party collection agency accepts payment by credit or debit card, they are also subject to the payment card industry data security standards.*
- ✓ *Third-party collectors are also subject to FDCPA.*
- ✓ *It is good practice to record all interactions and monitor frequently for compliance. Consider adding screen analytics applications that automatically tag and categorize recordings based on events that occurred during the call. They will help you quickly locate recordings that require review.*
- ✓ *If agents are not authorized to have access to certain identifiers, such as addresses or social security numbers, CEs and BAs should install software that automatically masks or encrypts this information.*

Family Medical Leave Act (FMLA)

The Family and Medical Leave Act provides certain employees with up to 12 workweeks of unpaid, job-protected leave a year, and requires group health benefits to be maintained during the leave. The law applies to all public sector employers and private sector employers at locations with 50 or more employees. Employees must have been on the job for at least 12 months and have worked for a minimum of 1250 hours. The law has recently been expanded to comply with the National Defense Authorization Act (NDAA) of 2008 to allow eligible employees of covered employers to take FMLA-qualifying leave “because of any qualifying exigency...arising out of the fact that the spouse, son, daughter, or parent is on active duty or has been notified of an impending call to active duty in the Armed Forces in support of a contingency operation.” The NDAA also provides that “an eligible employee who is spouse, son, daughter, or next of kin of a covered service member shall be entitled to a total of 26 workweeks of leave during a single 12-month period to care for the service member.”

FMLA creates scheduling difficulties for contact centers. Employees do not have to take time-off in consecutive days. The Act requires a 30-day advance notice for “foreseeable” absences but for unforeseeable leave, the Act applies an ambiguous “as soon as practicable” standard. There have been complaints by employers that employees use FLMA as a pretext for tardiness or as leverage to obtain a preferred shift.

Employees may choose to use, or employers may require the employee to use, accrued paid leave to cover some or all of the FMLA leave taken. Employees may choose, or employers may require, the substitution of accrued paid vacation or personal leave for any of the situations covered by FMLA. The

substitution of accrued sick or family leave is limited by the employer's policies governing the use of such leave.

Best Practice Tips

- ✓ *Large contact centers should work with their HR departments to estimate the impact of FMLA on attendance. Because of the high proportion of mothers with children, contact center management should prudently assume that FMLA-related time off will be higher in the contact center than other departments.*
- ✓ *The estimated impact of FMLA should be built into the shrinkage factor for workforce management software.*
- ✓ *Smaller contact centers with little or no provision for shrinkage should establish alternate relief options. For example, back office employees can be cross-trained for agent duties, relationships can be established with reliable outsourcers, or - if the contact center has the enabling technology - home agents can be contacted to pick up the slack. Today's web-based performance management technologies support home agents comparably to on-site agents.*
- ✓ *However, agent duties should not be turned over to untrained personnel. The risks of customer dissatisfaction and potential compliance violations are too great.*
- ✓ *FMLA time-off should be separately accounted for in the automated workforce management or manual scheduling system and reported to human resources.*
- ✓ *Management may request medical certification.*
- ✓ *Internal policies on time-off should be clearly spelled out and communicated to agent staff.*

To Learn More

This paper is a brief summary of hundreds of pages of legislation. Provided below is a list of web resources where you can find more detail on the subject of federal legislation and PCI-DSS compliance.

Information Sources

Federal Act	Website
PCI Compliance	http://www.pcicomplianceguide.org/
Telemarketing Sales Rule	http://www.ftc.gov/bcp/edu/pubs/business/marketing/bus27.shtm
TILA, Regulation Z	http://www.fdic.gov/regulations/laws/rules/6500-1400.html
FDCPA	http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre27.pdf
HIPAA Privacy Rule	http://www.cms.hhs.gov/MLNproducts/downloads/SE0726FactSheet.pdf
FMLA	http://www.dol.gov/esa/whd/regs/compliance/1421.htm

For state laws, the reader may wish to visit the web site of the American Teleservices Association (www.ATA.org). ATA publishes comprehensive guidebooks on both state and federal regulatory information (<http://www.ATA.regulatoryguide.com/ata.asp>). These include up-to-date information on consent-to-record laws. These documents must be purchased.

Summary

Whether your contact center is large or small, compliance has to be one of your most important priorities. We live in litigious times and the contact center -as the entrée' point to the enterprise - represents a highly visible target. With the proliferation of web sites and blogs, consumers are more informed about their rights than ever before. The Federal Trade Commission received 35,000 consumer complaints and inquiries in 2007. Only a tiny fraction of aggrieved consumers will actually communicate with the FTC, the Better Business Bureau, or contact the companies directly. Most will simply stop doing business with you, tell others about their unhappy experiences or worse yet - call an attorney. Noncompliance with consumer protection laws can be costly. The FTC meted out \$240 million in remedies between March 2007 and February 2008.

This paper highlights some of the most pertinent laws and regulations that impact the contact center. It is by no means comprehensive. The tips provided throughout can be summarized as:

- ✓ *Sensitivity to consumer privacy*
- ✓ *Avoidance of fraudulent and deceptive practices*
- ✓ *Training and preparation*
- ✓ *Sound practices to monitor and evaluate compliance*
- ✓ *Investments in the right technologies*

Technology plays an important role in compliance. We recommend that contact centers record and archive all voice and data interactions. Sensitive verbal and data recordings should be accessible only to authorized personnel. Your recording application should be able to quickly identify and retrieve potentially problematic interactions. Advanced speech and screen analytics tools are very valuable for this purpose, as you may not always know exactly what you are looking for.

Based on inquiries to the FTC and the volume of court cases, identity theft is the number one consumer fraud concern in the country. Virtually every enterprise of any size accepts credit or debit cards at some level. The payment card industry compliance solution developed by VPI Corporation provides the security and flexibility businesses need to help assure that sensitive card information does not leak out through the contact center.



About the Author

Dick Bucci is Senior Consultant for The PELORUS Group (www.pelorus-group.com) where he specializes in contact center technologies. He has authored eight in-depth reports on workforce optimization applications and numerous articles and white papers. Dick is also managing director of Technology Marketing Associates, a marketing consulting firm. He has over 30 years of experience in the telecommunications industry.

About VPI

VPI (Voice Print International, Inc.) is the premier provider of integrated interaction recording and workforce optimization solutions for enterprises, small- to medium-size businesses, trading floors, government agencies, and first responders. Through its award-winning suite of solutions, VPI empowers organizations to proactively improve the customer experience, increase workforce performance, ensure compliance, and align tactical and strategic objectives across the enterprise. With the power to be proactive, organizations are equipped to actively identify and maximize opportunities and minimize risk. For more than a decade, VPI has been providing proven technology and superior service to more than 1,000 customers in over 35 countries. For more information, visit <http://www.VPI-corp.com>.