HigherGround®

whitepaper

Call Recording and the Law
A Comprehensive Guide to Compliance and Best Practices

Prepared by Industry Analyst Dick Bucci
Senior Consultant, The PELORUS Group

TABLE OF CONTENTS

INTRODUCTION

The current legal landscape for call recording consists of numerous state and federal laws, along with industry mandates. These rules and regulations have been written primarily to protect individual rights to privacy and to protect individuals and businesses from fraud and abuse.

It is useful for contact center managers, among others, to have a common resource that offers useful guidance on best practices necessary to achieve and maintain both compliance and verification. "*Call Recording and the Law*" is based on public information, including the original acts, congressional amendments, FCC decisions, and state legislation. **This compendium is intended to be a useful resource but does not constitute legal advice. Readers are urged to consult their attorneys for legal advice.**

We have attempted to address the laws and other requirements that we believe impact the largest number of contact centers. These include:

- Consent-to-Record Laws
- Telemarketing Sales Rule
- Truth-in-Lending Act
- Fair Debt Collection Practices Act
- Verification and eDiscovery
- Payment Card Industry Compliance
- Privacy Rule - Heath Insurance Portability and Accountability Act (HIPAA)
- Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley)

This list is by no means comprehensive. There are literally hundreds of state and federal statutes covering privacy rights, banking, commerce, and labor with which contact centers must be compliant and/or familiar. Large public companies will likely have compliance officers who can provide this type of guidance. In smaller companies, however, you should have access to internal staff attorneys or outside counsel who are current on these isssues. It is in your interest to have at least a working knowledge of the laws that most directly effect contact center operations. This summary, based on extensive research, is meant to be a useful guide.

In general, this paper addresses federal legislation. Federal laws apply to interstate commerce. States typically enact their own legislation, modeled after the federal statutes, to ensure compliance for intrastate commerce. State laws can be more stringent than the federal laws.

Finally, the scope of this paper addresses rules within the United States only. There are also a myriad of privacy, commerce, and labor laws applicable in foreign countries addressing the issues of recording and data protection. Examples include:

- EU Data Protection Directive
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)

According to legal experts, the U.S. approach is more targeted - addressing specific industries or business activities like healthcare, banking, and debt collection. Other Western nations take a more sweeping view of privacy and protection against unfair business practices.

CONSENT-TO-RECORD

The legal right to record conversations between two or more parties, with or without the express consent of all parties, is addressed by both federal and state wiretapping laws. The laws apply to employees as well as outside callers. If the conversations take place completely within one state, then state laws prevail. Federal laws are aimed at interstate and international calls. Federal law (which permits monitoring with the consent of one party) does not pre-empt more restrictive state eavesdropping laws, even when the monitored communications are interstate. Accordingly, companies that monitor interstate calls for quality control purposes must consult the applicable provisions of state as well as federal law.

The Federal Electronic Protection Act permits the recording of telephone calls and in-person conversations only with the consent of at least one of the parties. Quoting from the applicable federal law, *"It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortuous act in violation of the Constitution or laws of the United States or of any state."*

This is called a "one-party consent" law. Under one-party consent, a participant can record a phone call or conversation so long as he/she is a party to the conversation. Furthermore, under federal law and some "one-party consent" state laws, the call may be recorded by a person not involved in the communication if one of the parties to the communication has given prior consent that the call be recorded, unless such communication is intercepted for the purpose of committing a crime.

Thirty-eight states and the District of Columbia have adopted one-party consent laws. The other twelve states, categorized as "two-party consent" states, require the consent of at least two parties to the call.

Assuming that the due process elements of jurisdiction are otherwise present, either the originating or terminating state of an interstate call may have a claim to jurisdiction over an eavesdropping complaint. Specifically, the state in which the call is monitored or recorded may claim jurisdiction because the monitoring occurred there, and the state in which the plaintiff resides may take jurisdiction because the harm to the victim occurred there. The laws of both the originating and terminating states must be taken into account before the decision to monitor or record a call between those states is made.

Federal law also applies in Commonwealth of Puerto Rico, as well as in any territory or possession of the United States.

One Party Consent States

Alabama
Alaska
Arizona
Arkansas
Colorado
District to Columbia
Georgia
Hawaii
Idaho
Indiana
Iowa
Kansas
Kentucky
Louisiana
Maine
Michigan
Minnesota
Missouri
Montana
Nebraska
New Jersey
New Mexico
New York
North Carolina
Ohio
Oklahoma
Oregon
Rhode Island
South Carolina
South Dakota
Tennessee
Texas
West Virginia
Wisconsin
Wyoming

Two Party Consent States

California
Connecticut
Delaware
Florida
Illinois
Maryland
Massachusetts
Nevada
New Hampshire
Pennsylvania
Vermont
Washington

The above listing is necessarily an over-simplification. There are many unique provisions in state laws. For example, the California statute prohibits the recording of confidential communications without "the consent of all parties." Evidence obtained in violation of this section may not be used in any judicial proceeding. This prohibition is confined to confidential communications, defined by statute as "*any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties there to,*" but does not include communications made under any "*circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.*"

The Connecticut statute creates a civil cause of action for any person whose telephone conversation is recorded unless the person recording the conversation received the "consent of all parties to the communication." **Consent must be obtained either in writing or orally at the beginning of the recorded conversation.**

Q. What constitutes "consent"?

A. Under the federal law consent may be explicit or implied. To achieve implied consent courts have held that it is sufficient to establish that the consenting party received actual notice of the monitoring and used the monitoring systems regardless. In Grigg-Ryan v. Smith the court held that "*Implied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.*"

Other cases have established that "proof of notice" to the distant party generally supports the conclusion that the party knew of the monitoring. A California court in Kearny v. Salomon Smith Barney stated "*If a business informs a client or customer at the outset of a telephone call that the call is being recorded, the recording would not violate the applicable state statute.*"

Q. Do the consent-to-record laws apply to employees as well?

A. In all-party consent states, employees must also consent to the recording or monitoring the content of communications. For example, a customer service representative should receive clear notice of any recording policy – either on each call or in writing beforehand – and, ideally, provide express, written consent to the policy.

TELEMARKETING SALES RULE

The Federal Trade Commission (FTC) issued the Amended Telemarketing Sales Rule (TSR) on January 29, 2003. The amended rule gives effect to the Telemarketing and Consumer Fraud and Abuse Act of 1994. The legislation gives the Federal Trade Commission and state attorneys general law enforcement tools to combat telemarketing fraud. It also provides consumers added privacy protection and defenses against unscrupulous telemarketers, and helps consumers identify the difference between fraudulent and legitimate telemarketing. The FTC defines Telemarketing as "*a plan, program, or campaign…to induce the purchase of goods or services or a charitable contribution involving more than one interstate call.*"

The FTC does not have jurisdiction over strictly intrastate telemarketing, although there are applicable state statutes:

- With a few exceptions, the TSR applies to any business or individual that takes part in "telemarketing." The calls may be inbound or outbound. The TSR is not limited to telesales personnel. Virtually any business or individual that offers for sale or arranges for the sale of goods or services via the telephone or solicits on behalf of a charitable organization is subject to the TSR.
- The following businesses are not covered by the TSR, but may be covered by others laws and regulations:
  - Banks, federal credit unions, and federal savings and loans.
  - Common carriers such as long distance telephone companies and airlines when they are engaging in common carrier activities.
  - Non-profit organizations. However, third-party for-profit organizations retained by these organizations to raise funds or solicit business are covered by the rule.
- Calls that are exempt:
  - Unsolicited calls from consumers that are not in response to a solicitation such as hotel reservations, restaurant reservations, and take-out orders.
  - Calls placed by consumers in response to a catalog.
  - Business-to-business calls that do not involve retail sales of nondurable office supplies such as paper, pencils, cleaning supplies, solvents and other items that may be depleted during the ordinary course of business.
  - Calls made in response to general media advertising (with some exceptions).
  - Calls made in response to direct mail advertising (with some exceptions).
  - Calls that are part of transactions involving face-to-face sales presentations.

Material Disclosures

The rule requires sellers and telemarketers to provide certain material information before the consumer pays for the goods or services that are the subject of the sales offer. "Material" information is information that would likely effect a person's choice of goods or services or the person's decision to make a material contribution.

- The material information must be provided in a "clear and conspicuous" manner.
- The material information must be provided prior to securing the consumers consent to purchase or arranging for courier pick up of payment.
- The information may be provided orally or in writing. When disclosures are oral, they must be clear and conspicuous and expressed at an understandable speed and pace and in the same tone and volume as the sales offer.
- Material information includes:
  - The full cost to purchase, receive, or use the offered goods or services, including the number and amount of installment payments.
  - The total quantity of goods or services the consumer purchases or receives.
  - Any conditions or limitations associated with the offer. Examples are cash payment, prior deposit to secure a credit card, and limitations on the use of vacation certificates.
  - Information on refund, cancellations, and exchanges – but only if these policies are mentioned in the sales presentation.
  - If the policy is "all sales are final'" then this information must be clear and conspicuous, orally or in writing.
  - Special disclosures required for prize promotions, credit card loss protection plans.
  - "Negative options" where the seller interprets the consumer's absence of a clear decline as acceptance of the offer, for example "free trials." The seller must explain that the buyer's account will be charged unless the buyer takes some affirmative action like canceling the order or subscription.

Mandatory Disclosures In Outbound Sales Calls And Up-Selling Transactions

- The telemarketer or seller must **promptly** disclose the following information:
  - The identity of the seller. This refers to the name of the organization, not the name of the individual agent.
  - That the purpose of the call is to sell goods or services.
  - The nature of the goods or services offered for sale.

- In the case of a prize promotion, it must be explained that no purchase or payment is required to participate or win, and that a purchase or payment does not increase the chances of winning.

Special Rules For Up-Sells

- The same rules (above) apply to up-sells if any of the information is different from the original disclosures.
- In an **external** up-sell, where the second transaction in a single telephone call involves a second seller, the consumer must be told the identity of the second seller.
- In an **internal** up-sell, where additional goods or services are offered by the same seller in the same transaction, no new disclosure of the seller's identity is required, as that information is already known.

Misrepresentations Are Prohibited

The rule prohibits sellers and telemarketers from making false or misleading statements to induce anyone to pay for goods or services or make a charitable donation.

Express Verifiable Authorization

Express verifiable authorization (EVA) is required when payment is made by methods other than a credit or debit card. These types of payments are covered by other regulations. The rule does not apply to money orders and mailed checks but does apply to "phone checks" and other unconventional payment methods. With a phone check the seller collects routing and account information from the consumer and charges his/her checking account. The seller is required to obtain an EVA even if a third party is responsible for processing the phone payment. The third party may also be held liable if it substantially assists the seller in processing payments and knows – or consciously avoids knowing – that seller is failing to collect the EVA.

Under the rule, authorization is considered verifiable if it is obtained in one of three ways:

- Advance written authorization from the consumer.
- An **audio recording** of the consumer giving express verifiable authorization.
- Written confirmation of the transaction is sent to the consumer before charges are submitted for payment.

The rule requires sellers to maintain a record of all verifiable authorizations.

Recorded Authorizations
An audio recording of an oral authorization for payment must clearly demonstrate that the consumer has received seven specific pieces of information about the transaction and the consumer has authorized that funds be taken from or charged to his or her account:

- The number of debits, charges or payments.
- The date the debits, charges, or payments will be submitted for payment.
- The amount of the debits, charges, or payments.
- The customer or donor's name.
- The customer or donor's billing information, including which account will be used for the transaction.
- A telephone number that is answered during normal business hours.
- The date of the consumer's oral authorization.

The rule also requires that recorded oral authorizations be made available upon request to the customer or donor, as well as the customer or donor's bank or other billing entity. Silence or some other ambivalent response is not deemed consent under the rule. Consent must be affirmatively and unambiguously expressed.

Special Rules For Pre-Acquired Account Information
In some cases telemarketers and sellers will already have consumer account information prior to initiating a telephone sales transaction. In that event, the telemarketer or seller **must** secure the following information to execute the sale:

- Obtain from the seller the last four digits of the account number to be charged. It is not required that the seller have access to the buyer's account information to verify that these are the correct four digits. Telemarketers should not have access to private consumer account information.
- Obtain the consumer's express agreement to be charged using the identified account information.
- **Make and maintain an audio recording of the entire transaction.**

Recordkeeping
The rule requires telemarketers and sellers to keep records of all verifiable authorizations except those paid for by check, credit card, or debit card. If authorization is via audio recording, **a copy of the recording must be maintained**. The recording must include all information disclosed to the consumer as well as the consumer's oral authorization.

Q. Which entity is responsible for enforcing the Telemarketing Sales Rule?
A. The Federal Trade Commission (FTC).

Q. Does the TSR apply only to telemarketers?
A. No. The TSR defines three categories of telephone sales workers: telemarketers, telefunders, and sellers.

Q. Does the TSR apply to offshore outsourcers?
A. Yes, if they are originating or receiving calls from U.S. residents.

Q. Does the TSR apply to up-sells and cross-sells?
A. If an agent attempts to up-sell the caller to a product or service that was not the object of the initial consumer contact then the up-sell portion of the call is subject to the TSR, even if the original query was exempt. The FTC is silent on the subject of cross-sells but it is prudent to assume that the same rules apply.

Q. Does the TSR mandate call recording?
A. Only in one situation – sales made to consumers where the seller has pre-acquired account information. Otherwise, recording is solely for the purposes of quality control and proving compliance.

Q. Do the mandatory disclosures apply to survey calls, such as customer satisfaction surveys?
A. The mandatory disclosures are only required if the person conducting the survey plans to move into a sales presentation during or after the survey call. The same applies to new customer greeting calls.

Q. What is the penalty for violation of the TSR?
A. The penalty is $11,000 per violation. For example, under the terms of a consent order Special Data Processing Corporation (SDP) of Clearwater, Florida, agreed to pay the Federal Trade Commission $535,000 as compensation to consumers to resolve charges that it misled them about the Triad Discount Buying Service (Triad) it sold to consumers.

In addition to a fine, violators may be subject to nationwide injunctions that prohibit certain conduct. Violators may be required to remedy harm caused to injured consumers.

TRUTH-IN-LENDING ACT

The Truth in Lending Act (TILA) was enacted on May 29, 1968 as Title 1 of the Consumer Credit Protection Act. Regulation Z, which gives effect to the provisions of TILA, became effective July 1, 1969. TILA was first amended in 1970 to prohibit the distribution of unsolicited credit cards to consumers. It has since been amended several times. TILA is a United States federal law designed to protect consumers in credit transactions by requiring clear disclosure of key terms of the lending arrangement and all costs associated with the transaction. TILA standardizes the manner in which costs associated with borrowing are calculated and disclosed. TILA 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.

With the exception of certain high-cost mortgage loans, TILA does not regulate the charges that may be imposed on consumers for the use of consumer credit. Rather, it requires uniform or standardized disclosure of costs and charges so that consumers can compare credit costs.

TILA applies to all entities that extend open-end or closed-end credit financing to consumers. Open-end credit refers to credit cards, charge cards, home equity lines of credit, and other instruments that do not have fixed installment schedules leading to payoff. Closed-end credit includes auto loans, home mortgages, personal loans, and other facilities that do have fixed repayment schedules.

TILA does not apply to commercial loans, loans to government entities, credit in excess of $25,000 not secured by real property, student loans, and securities brokers.

Material Disclosures

TILA provides very specific disclosure requirements for lenders. Examples include the methods by which interest rates are calculated, disclosure of the annual percentage rate, cost of late fees, terms, advance notice of renewals, and many other items consumers should be aware of when evaluating the cost and terms of credit. There are also rules governing the information that must be disclosed in advertising.

The original act and subsequent amendments are largely focused on written disclosure requirements, such as contract language and advertising. Regarding telephone solicitations, the act requires the following oral disclosures:

- Annual percentage rate applicable to extensions of credit under the credit plan.
- Where an extension of credit is subject to a variable rate, the fact that the rate is variable, the annual percentage rate in effect at the time, and how the rate is determined.
- Where more than one rate applies, the range of balances to which each rate applies.
- Any annual fee, other periodic fee, or membership fee imposed for the issuance or availability of a credit card, including any account maintenance fee or other fee charge imposed based on activity or inactivity during the billing cycle.
- Any minimum finance charge imposed for each period during which any extension of credit which is subject to finance charge is outstanding.
- Any transaction charge imposed in connection with use of the card to purchase goods or services.
- The date by which or the period within which any credit extended under such credit plan for purchase of goods or services must be repaid to avoid incurring a finance charge, and, if no such period is offered, such fact shall be clearly stated.
- If the length of such grace period varies, the card issuer may disclose the range of days in the grace period, if the disclosure is identified as such.
- The name of the balance calculation method used in determining the balance on which the finance charge is computed if the method used has been defined by the Federal Reserve Board, or a detailed explanation of the balance calculation method if the method has not been so defined.

However, none if this applies if any one of the following conditions is met:

- If the card issuer does not impose any fee as described in the act.
- If the card issuer does not impose any fee in connection with telephone solicitations unless the consumer accepts the terms by actually using the card.
- The card issuer discloses clearly and conspicuously in writing the above information within 30 days after the consumer requests the card, but in no event later than the delivery of the card, and the card issuer discloses clearly and conspicuously that the consumer is not obligated to accept the card or account and the consumer will not be obligated to pay any of the fees or charges disclosed unless the consumer elects to accept the card or account by using the card.

Q. Which government entity is responsible for creating Regulation Z of the Truth-in-Lending Act?
A. The Federal Reserve Board.

Q. Which government entity is responsible for enforcing the Truth-in-Lending? Act as it applies to banks?
A. Comptroller of the Currency.

Q. Does TILA apply only to credit card issuers?
A. No, it applies to all entities that extend credit facilities to consumers.

Q. What are the penalties for noncompliance?
A. If a creditor fails to comply with any requirements of TILA, other than the advertising provisions, it may be held liable to the consumer for actual damages and the cost of any legal action together with reasonable attorney's fees in a successful action.

If the creditor violates certain requirements of TILA, the creditor may also be liable for either of the following:

- In an individual action, twice the amount of the finance charge involved, but not less than $100 or more than $1,000.

- In a class action, such amount as the court may allow, but not to exceed $500,000 or 1 percent of the creditor's net worth, whichever is less. Individual violators will be fined not more than $5,000 or imprisoned for not more than one year, or both.

Fair Debt Collection Practices Act

The Fair Debt Collection Practices Act (FDCPA) which became effective March, 1978 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. Such practices can cause substantial consumer injury, including payment of amounts not owed, unintended waiver of rights, invasions of privacy, and emotional distress.

Although the Federal Trade Commission (FTC) is vested with primary responsibility under the FDCPA, it shares responsibility with seven other federal agencies. The FTC receives most of its information about violations directly from consumers. In 2006, the FTC received 69,204 complaints about third-party debt collectors. Another 21,425 complaints were received about in-house collectors. Total collection complaints, both third-party and in-house, totaled 90,629 in 2006 or 26% of all complaints received by the FTC. Over 40% of complaints were for demanding larger payments than required by law.

In November, 2007 the FTC obtained the largest civil penalty ever in a FDCPA case, $1.375 million from LTD Financial Services, L.P.

The FDCPA is primarily aimed at third-party debt collectors. For the most part, creditors are exempt from these rules when they are collecting their own debts.

Mandatory Disclosures

- Any debt collector communicating with any person other than the consumer for the purpose of acquiring location information about the consumer shall identify himself, state that he is confirming or correcting location information concerning the consumer; and, only if expressly requested, identify his employer.
- In the initial oral communication, the debt collector must state that he/she is attempting to collect a debt and that any information obtained will be used for that purpose.

Acquisition Of Location Information

- Any debt collector communicating with any person other than the consumer for the purpose of acquiring location information about the consumer shall not state that such consumer owes any debt.
- Shall not communicate with any such person more than once unless requested to do so by such person or unless the debt collector reasonably believes that the earlier response of such person is erroneous or incomplete and that such person now has correct or complete location information.

Communication In Connection With Debt Collection

- Without the prior consent of the consumer given directly to the debt collector or the express permission of a court of competent jurisdiction, a debt collector may not communicate with a consumer in connection with the collection of any debt at any unusual time or place or a time or place known or which should be known to be inconvenient to the consumer. In the absence of knowledge of circumstances to the contrary, a debt collector shall assume that the convenient time for communicating with a consumer is after 8 o'clock antemeridian and before 9 o'clock postmeridian, local time at the consumer's location.
- If the debt collector knows the consumer is represented by an attorney with respect to such debt and has knowledge of, or can readily ascertain, such attorney's name and address, all contacts must be with that attorney unless the attorney fails to respond within a reasonable period of time to a communication from the debt collector or unless the attorney consents to direct communication with the consumer; or
- At the consumer's place of employment if the debt collector knows or has reason to know that the consumer's employer prohibits the consumer from receiving such communication.
- Except as provided in section 804, without the prior consent of the consumer given directly to the debt collector, or the express permission of a court of competent jurisdiction, or as reasonably necessary to effectuate a post-judgment judicial remedy, a debt collector may not communicate, in connection with the collection of any debt, with any person other than a consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector.

Ceasing Communication

- If a consumer notifies a debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes the debt collector to cease further communication with the consumer, the debt collector shall not communicate further with the consumer with respect to such debt, except:
  - to advise the consumer that the debt collector's further efforts are being terminated;
  - to notify the consumer that the debt collector or creditor may invoke specified remedies which are ordinarily invoked by such debt collector or creditor; or
  - Where applicable, to notify the consumer that the debt collector or creditor intends to invoke a specified remedy.

Harassment Or Abuse

- A debt collector may not use any false, deceptive, or misleading representation or means in connection with the collection of any debt. Examples include:
  - The false representation or implication that the debt collector is vouched for, bonded by, or affiliated with the United States or any State, including the use of any badge, uniform, or facsimile thereof.
  - The false representation of the character, amount, or legal status of any debt.
  - The false representation or implication that any individual is an attorney or that any communication is from an attorney.
  - The representation or implication that nonpayment of any debt will result in the arrest or imprisonment of any person or the seizure, garnishment, attachment, or sale of any property or wages of any person unless such action is lawful and the debt collector or creditor intends to take such action.
  - The threat to take any action that cannot legally be taken or that is not intended to be taken.
  - The false representation or implication that a sale, referral, or other transfer of any interest in a debt shall cause the consumer to lose any claim or defense to payment of the debt.
  - The false representation or implication that the consumer committed any crime or other conduct in order to disgrace the consumer.
  - Communicating or threatening to communicate to any person credit information which is known or which should be known to be false, including the failure to communicate, that a disputed debt is disputed.
  - The use of any false representation or deceptive means to collect or attempt to collect any debt or to obtain information concerning a consumer.
  - The use of any business, company, or organization name other than the true name of the debt collector's business, company, or organization.
  - The false representation or implication that documents are not legal process forms or do not require action by the consumer.
  - The false representation or implication that a debt collector operates or is employed by a consumer reporting agency.

Unfair Practices

- A debt collector may not use unfair or unconscionable means to collect or attempt to collect any debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:
  - The collection of any amount (including any interest, fee, charge, or expense incidental to the principal obligation) unless such amount is expressly authorized by the agreement creating the debt or permitted by law.
  - The acceptance by a debt collector from any person of a check or other payment instrument postdated by more than five days unless such person is notified in writing of the debt collector's intent to deposit such check or instrument not more than ten or less than three business days prior to such deposit.
  - The solicitation by a debt collector of any postdated check or other postdated payment instrument for the purpose of threatening or instituting criminal prosecution.
  - Depositing or threatening to deposit any postdated check or other postdated payment instrument prior to the date on such check or instrument.
  - Causing charges to be made to any person for communications by concealment of the true purpose of the communication. Such charges include, but are not limited to, collect telephone calls and telegram fees.

Q. What debts are covered by the FDCPA?
A. Personal, family, and household debts; including money owed for an automobile, for medical care, or charge accounts.

Q. What action can consumers take to stop collector contacts?
A. Consumers can write a letter to the collection agency. Once the agency receives the letter it may not contact the debtor again except to say there will be no further contact or the creditor intends to take other specific actions.

Q. What actions can consumers take if they believe there has been a violation of the act?
A. Consumers may sue the debt collector in state or federal court. If successful, the debtor may recover money for damages suffered plus an additional $1,000. Court costs and attorney's fees may also be recovered. In class action suits plaintiffs may recover up to $500,000 or 1 percent of the collector's net worth, whichever is greater.

Q. Does the FDCPA require that telephone communications be recorded?
A. No, but there is no other way to establish compliance.

VERIFICATION AND E-DISCOVERY

Every day billions of dollars of transactions are completed or negotiated by telephone. Transactions range from $10 donations to local public television stations to sensitive multi-billion dollar corporate acquisitions. While fax and email have their places in business communications, telephone is second only to face-to-face for resolving disputes and forging agreements. In a world where speed is of the essence, buyers and sellers may be anywhere in the world, and air travel is both costly and increasingly unreliable, telecommunications has taken on greater prominence as the most practical and efficient means of communication.

Traditional consumer-focused call center agents generally have little or no authority to negotiate agreements. If a promise was made in error, the cost of granting the concession – even if unauthorized – is usually not significant. However, this is not the case with many other business functions that rely on the telephone for gathering critical information and negotiating agreements. Think of insurance claim agents taking accident reports by phone. Agent errors or intentional deceptions from the claimant can have significant impact on final settlements. Absent any more information than the data entered on the claim form, it is difficult, if not impossible, to prove which party is correct.

Another example occurs in the purchasing department. Buyers spend much of their days negotiating prices, quantities, and delivery schedules by phone. Telephone agreements are typically confirmed by fax or mail, but what if the paper confirmation does not match the buyer's notes or recollections of what actually transpired during the telephone call? How do you prove which party's version of the truth is correct? In environments like financial trading floors, where large transactions are handled by telephone and there is little time to wait for hard copy verification, **all calls are recorded to serve as proof of the transaction**.

It is easy to think of other situations where verification could be valuable. Prospective employees are typically interviewed first by telephone. Based on the results of the telephone call, a personal interview may be scheduled. What if an applicant later claims discrimination, based on alleged telephone questions about the applicant's age, sex, race, or disability? If the call was not recorded, who is to say that discrimination did not take place? Other departments that may benefit from call recording are accounts receivable/collections, legal, and investor relations. In the case of recording conversations between attorneys and clients, even in-house, there remains an issue of attorney-client priviledge and confidentiality which must be vigorously upheld.

Progressive businesses are extending their recording capability beyond the contact center. This is done by directing all incoming calls to the main number. The VRU/auto attendant takes the calls, plays the "this call may be recorded…" announcement, and then directs the call to the intended party. Of course, not all calls are recorded, but individuals that have need for verification have the ability to activate the recording function.

Federal Rules Of Civil Procedure

Electronic discovery is the process of obtaining, reviewing and producing digitally stored evidence in response to litigation or regulatory requests. It is estimated that 90% of business documents today are created and stored digitally. Emails comprise 70% of this digital documentation. In December 2006, the Federal Rules of Civil Procedure were amended to make clear that electronic data is subject to discovery if it is relevant and not burdensome to produce. Rule 34 applies to "*information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined.*"

Although Rule 34 is clearly aimed at emails, the definition of electronically stored information (ESI) is intentionally broad and clearly encompasses voicemails and other **recorded voice interactions**. The Rule covers information "*stored in any medium.*" Either party to litigation can subpoena ESI, subject to some limitations, including pertinence to the case, privacy protections and the practical ability to retrieve the information. The requesting party may designate the forms or form in which it wants ESI produced.

Litigants may request call center interactions as well as voicemails. It is much easier to retrieve voice interactions from **full recording systems** then telephony voicemails systems, especially when coupled with speech analytics tools. Organizations should consider supplementing enterprise voicemail with user-enabled interaction recording.

A recent study reports that 24% of employers have had email subpoenaed by courts and regulators, while another 15% have battled lawsuits triggered by employee email.

PAYMENT CARD INDUSTRY COMPLIANCE

Identity theft is one of the fastest growing crimes in America and the world. According to an exhaustive study funded by the Federal Trade Commission, 8.3 million people - or about one out of 25 adults - were victimized by identify theft in 2005. Estimated losses were $15.6 billion. The three major sources of fraud were new accounts, misuse of account numbers, and misuse of credit cards and credit card account numbers. While most victims report small or no out-of-pocket costs, one out of ten incurred expenses of at least $3,000 and spent at least 55 hours of their own time resolving problems like replacing lost documents or restoring damaged credit ratings.

In December, 2006 TJX Companies, which is made up of several popular retailers including TJ Maxx and Marshall's, admitted that hackers placed software on the company's network to capture data from at least 45.7 million customer credit and debit cards. Some numbers were used to make fake credit cards, which law enforcement authorities said were used to buy millions of dollars in expensive electronics from Wal-Mart and other retailers in Florida and elsewhere. According to the Boston Globe, several analysts estimated TJX's costs could run as high as $1 billion, including legal settlements and lost sales.

So what does all this have to do with call centers? Actually - a lot. Call center agents, particularly those tasked with generating revenue, often have access to personal information such as credit and debit card numbers, banking accounts, and social security numbers. A British newspaper investigation revealed that customer details, including bank accounts, passport numbers, mobile numbers, and even medical records can be bought from poorly paid Indian call center workers for small amounts of cash. The paper reported that its investigator was able to buy financial details of 1,000 people for only $5 per contact.

To combat identity fraud the major card issuers including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, formed the Payment Card Industry Security Standards Council (PCI-DSS). The council is responsible for issuing and maintaining industry-wide data security standards. Previously, each card issuer had its own standards. The data security standard (PCI-DSS) is freely available (https://www.pcisecuritystandards.org). Enforcement is via contracts signed with the card issuer. 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. The card issuers can fine companies for non-compliance and suspend privileges to use their cards to accept payment.

Early in 2007 Minnesota became the first state to codify certain requirements of the PCI-DSS. Under the state's new Plastic Card Security Act, any company that suffers a data breach and is found to have been storing prohibited card data on its systems will have to reimburse banks and credit unions for the costs associated with blocking and reissuing cards. Such companies could also be subject to private action brought by individuals who might have been affected by a violation of the state law.

Companies handling fewer than 20,000 payment card transactions per year are not liable under the law. Other states have pending legislation. At the federal level, Senator Patrick Leahy (D-VT) has sponsored the Social Security Number Misuse Prevention Act. This act, if passed, will amend the Federal Criminal Code to prohibit the display, sale, or purchase of Social Security numbers without the affirmatively expressed consent of the individual, except in specified circumstances.

Payment card industry standards are just one of many industry and regulatory initiatives intended to protect personal identity. Contact center managers and employees need to be aware of the requirements that apply specifically to their environments and must have a program for achieving compliance. At a minimum the program should include:

- In depth reviews with in-house IT staff and compliance officials.
- Examination of pre-employment screening practices.
- Research into technologies and applications that encrypt or conceal sensitive information.
- Exploring ways to confirm caller identity without requiring protected information.
- If outsourcers are used, they must be compliant with applicable requirements and rigorous in hiring practices and internal security.
- Changes to all default passwords.
- Have a clear written policy regarding the processing of credit/debit cards and be sure everyone understands it.

The contact center is only one function in the enterprise that may have access to protected information. Compliance initiatives need to address the enterprise as a whole.

Q. What is the penalty for noncompliance?
A. Companies that do not comply with the requirements face penalties as high as $500,000.

Q. What is the legal authority for the Payment Card Industry to force compliance and issue penalties?
A. The authority rests with the individual contracts required by each card issuer.

Q. Do the PCI standards apply to all companies that accept payment cards?
A. Yes, if they accept Visa or MasterCard. These issuers provide four levels of compliance, depending on the number of annual transactions. Level 4 (6million transactions or more) require an annual onsite audit and quarterly network scans. Lower level merchants need only complete and submit self-assessments as well as the quarterly network scans.

PRIVACY RULE - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The stated intent of the Heath Insurance Portability and Accountability Act of 1996, better known as "HIPAA," is "*To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.*"

The legislation provides several specific consumer protections with regard to health care. The act:

- Limits the use of pre-existing condition exclusions;
- Prohibits most group health plans from discriminating by denying coverage or charging extra for coverage based on an individual's or family member's past or present poor health;
- Guarantees certain small employers, and certain individuals who lose job-related coverage, the right to purchase health insurance; and
- Guarantees, in most cases, that employers or individuals who purchase health insurance can renew the coverage regardless of any health conditions of the individuals covered under the insurance policy.
- Established standards for electronic data interchange and transactions.
- Established standards for the protection of personal health information.

The Department of Health and Human Services (HHS) is principally responsible for administering and enforcing HIPAA. The Office of Civil Rights (OCR) is responsible for enforcement. Violations and enforcement actions are complaint-driven. OCR does not have the staff to go out on site looking for violations. Patients may file complaints with their service providers or the OCR.

Important Terms

Individually Identifiable Health Information
This refers to health information that could be reasonably traced to a specific individual. Examples include:

- Past, present or future physical or mental health conditions.
- The provision of health care to the individual.
- The past, present, or future payment for the provision of health care to an individual.
- Demographic data and common identifiers like name, address, birth date, and social security number.

PHI – Protected Health Information
The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form of media, whether electronic, paper, or oral. The Privacy Rule calls this "*protected health information*" (PHI).

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, heath care clearinghouses, and health insurers, among others.

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 (if they have access to PHI). BAs must also agree to the privacy and data security requirements of HIPAA.

The Privacy Rule

HIPAA mandated the Department of Heath and Human Resources to establish standards for electronic data interchange and transactions and privacy protection for individual health information. In response to the latter, HHS published the Privacy Rule which became effective April 14, 2001. The Rule set national standards for the protection of health information, as applied to three types of "*covered entities*" – health plans, health care clearing houses, and health care providers who conduct certain health care transactions electronically.

In August, 2002 HHS published modified rules. The current rule went into effect on April 14, 2003. A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be shared. The Privacy Rule requires health plans, pharmacies, doctors, and other covered entities to establish policies and procedures to protect the confidentiality of protected health information about their patients. Important elements of the Privacy Rule include:

- Patients must have access to their medical records. Medical records may be on paper, in computers, or communicated orally.
- CEs must provide notice to patients of how they plan to use patient medical records.
- CEs must provide notice to patients of their rights under the privacy regulation.
- PHI generally may not be used for non-medical purposes.
- CEs may share only the minimum information required for a particular purpose.
- CEs must first secure permission from patients before using PHI for marketing purposes.
- Doctors must honor patient requests for confidentiality, such as requesting calls to his/her office rather than home.
- CEs must establish policies and procedures to assure confidentiality of PHI.
- CEs must train their employees in privacy procedures and designate an individual responsible for making sure the procedures are followed.
- CEs must take steps to assure that BAs agree to the same limitations as the CE. Formal agreements are required. HHS provides model contract language.
- Consumers may file formal complaints regarding privacy practices of covered entities.
- Rules apply to both private business and government entities.

The HIPAA privacy standards do not pre-empt state laws that have the same or stronger requirements. The privacy standards are cumulative.

Implications For Interaction Recording

Outsourcers – Health care providers often use third party contact centers. Typical applications are bill collections and patient recruitment for clinical testing. In those cases, the third party will almost certainly have access to PHI (even patient names and phone numbers qualify). The outsourcer must sign a Business Associate agreement. Model agreements recommended by HHS have many provisions. Included among these are that the:

- BA agrees to not use or disclose PHI created or received from or on behalf of CE other than permitted or required by the agreement or as required by law.
- BA agrees to report to CE any use or disclosure involving PHI it receives from, or on behalf of the CE that is not provided for by this agreement of which it becomes aware.
- BA agrees to report to CE any security incident involving ePHI of which it becomes aware. (Note: Recorded voice would be considered electronic protected health information or "ePHI".)
- BA agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of PHI received from, or created or received BA on behalf of CE, available to the Secretary of HHS for the purpose of determining CE's compliance with the Privacy Rule.
- BA agrees to document disclosures of PHI and information related to such disclosures as would be required for CE to respond to a request by and individual for an accounting of disclosures.

Internal service centers and help desks – Firms involved in health care are major employers of contact center agents. Insurance (all types) is the second largest employer type with over 130,000 agents. As covered entities, the privacy requirements are more stringent than for outsourcers. **Full recording of all interactions (both voice and data) should be standard practice** and should be included in the formal policies and procedures adopted by the CE to assure compliance.

Q. How should CEs determine the minimum necessary information that can be used, disclosed, or requested for a particular purpose?
A. The Office of Civil Rights directs CEs must "*make their own assessment of what protected health information is reasonably necessary for a particular purpose.*"

Q. Are business associates subject to regulation by HHS?
A. No, the BAs obligations are contractual, not regulatory.

Q. Are archived interaction recordings considered protected health information?
A. Not unless they include individually identifiable health information. If they do, then the recordings are considered electronic PHI and must be treated with the same care as other PHI, as spelled out in the CEs policies and procedures.

Q. Are collections agencies working on behalf of health care providers still subject to the Fair Debt Collection Practices Act?
A. Yes.

Q. Are there exemptions for small practices?
A. The Privacy Rule applies to all covered entities, regardless of size. The flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment.

Q. What are the penalties for violation?
A. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year.

HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

A person who knowingly obtains and discloses individually indentifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if wrongful conduct involves false pretenses, and up to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use of individually identifiable health information for commercial advantage, personal gain, or malicious harm.

PUBLIC COMPANY ACCOUNTING REFORM AND INVESTOR PROTECTION ACT (SARBANES-OXLEY)

The Public Company Accounting Reform and Investor Protection Act of 2002 and commonly called "SOX" or "Sarbox" is a United States federal law enacted on July 30, 2002 in response to a number of major corporate and accounting scandals. The stated goal of the Act is *"To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."*

SOX, as we will refer to it here, applies only to companies regulated by the United States Securities and Exchange Commission. Privately held companies are not affected by SOX. Further, the requirements are not as onerous for companies with less than $75 million in public equity float. SOX is highly complex legislation, consisting of eleven sections. Principal outcomes of the legislation include:

- The establishment of the Public Company Accounting Oversight Board, to oversee the audit of public companies that are subject to the securities laws.
- Reduction of potential conflicts of interest between public accounting firms and their auditing clients by prohibiting or constraining the contemporaneous marketing of specified non-auditing services.
- Mandatory 5-year rotation of accounting firm partners responsible for conducting a firm's audit.
- The principal executive officer or principal financial officer of a publicly held company must certify the authenticity and accuracy of SEC-mandated financial reports by personally signing off on them, and assuming personal liability for their accuracy.
- Prohibition of insider trading during pension fund blackout periods.
- Public disclosure of off-balance sheet transactions.
- Prohibitions on personal loans to directors and corporate executives.
- Auditors must prepare an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the public company being audited.
- Public companies shall disclose to the public on a rapid and current basis such additional information concerning material changes in their financial condition.
- Elimination of conflicts of interest on the part of financial analysts.
- Criminal penalties of up to 20 years imprisonment for the destruction of documents and other attempts to impede investigations by the SEC.
- Whistleblower protection for employees that come forward with information to help an existing or initiate a new SEC investigation.
- Criminal penalties for defrauding shareholders.

- Extension of power of SEC to prohibit persons who have violated certain provisions of SEC laws and regulations from serving as corporate officers or board members.
- Any accountant who conducts an audit of an issuer of securities shall maintain all audit or review work papers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.

Supporting documentation for an audit could potentially include faxes, voicemail, e-mail, and written communications. After July 26, 2003 organizations were required to file and report electronic records, including e-mails. Organizations that have not already done so should implement an email retention program and the operating systems necessary to restore and retrieve emails for 5 years or longer. It is not necessary to save every deleted and sent email produced by every employee, but employees should not be left to decide on their own which email messages should be saved and which should not.

Implications For Interaction Recording

Recorded voice, whether archived as voicemail or contact center interactions, is electronic information and subject to audit and investigation. However, voicemail only captures interactions that were not completed. As well, voicemail is difficult to search and retrieve, since it was not designed for that purpose. **Public companies and auditing firms should consider extending full recording to sensitive business functions and to the entire auditing process.** Most states require only one-party consent to record calls. In any event, the firms can always terminate incoming calls via an auto-attendant where the standard "This call may be recorded…" message is provided to all callers prior to connecting the call to the desired party. Recording can then be activated on demand, as the nature of the call warrants.

Contact centers

Post-Arthur Andersen and SOX, auditing firms have become extra vigilant. Every business function, including the contact center operation, should expect to be carefully audited. Contact center managers must be prepared to share all documentation pertaining to departmental standards, expectations, and benchmarking. This will likely include job descriptions, organization charts, evaluation forms, complaint handling procedures, training, benchmarking, and privacy protections.

Investor relations

Prudent pubic companies are well advised to record all interactions between investor relations personnel and outside investors. These interactions can then be periodically reviewed for accuracy and integrity.

Sales departments
Sales executives often negotiate large contracts by phone. As an internal control measure, it may be prudent to instruct sales personnel to record these calls. This action provides an indisputable record of what was agreed to and provides management with a tool to track down potentially suspect agreements.

Auditing firms
For their own protection, auditing firms may find it wise to record all telephone interactions between their clients conducted during annual audits.

Finance departments
For the same reason, finance departments may wish to record and spot-check communications between their employees and independent auditors.

Investment firms
Investment firms should consider recording calls between analysts and the companies they cover. This would help spot potential conflicts of interest.

Q. What does it cost a company to comply with Sarbanes-Oxley?
A. A survey sponsored by Finance Executives International (FEI) indicated that 200 companies with average revenues of $6.8 billion spent an average of $2.9 million, in 2006 complying with SOX.

Q. Which government entity has primary responsibility for SOX?
A. The United States Securities and Exchange Commission.

Q. Does SOX directly address contact centers?
A. There are no specific references to contact centers. The contact center has the same responsibilities as other business functions.

Q. When will the requirements for smaller companies be in place?
A. The SEC has issued amendments for smaller companies, defined as those with less than $75 million in public float, to relieve them of some of the more burdensome disclosure requirements. The amendments have different effective dates, from February 8, 2008 to March 15, 2009. For more detail see http://www.sec.gov/rules/final/2008/33-8876fr.pdf. These are amendments to the current rules. Smaller companies are currently covered by SOX.

Q. What are the penalties for violation?

A. The penalties vary depending on which provision is violated, but can be very severe. For example, executives that willfully certify the accuracy of SEC-filed reports knowing at the time that they were in violation of provisions of the Act can be fined up to $5 million and sentenced to up to 20 years in federal prison.

SUGGESTED BEST PRACTICES

Consent to record

- On inbound calls always provide an announcement, such as "This call may be recorded for quality and training purposes" if there is a possibility the call will be recorded.
- When receiving calls from states that require prior express consent, such as Connecticut, request the caller's permission to be recorded. Record both the announcement and the caller's response. If the distant party declines permission, then the agent needs to be able to manually override the recording process. If possible, program the IVR to add a menu selection that is activated only when calls are received from a prior-consent state like Connecticut. The IVR will speak the recorded announcement then ask the caller to press a key to signify permission to be recorded. If this can't be done automatically, then automatic recording should be turned off, based on the area code of the incoming call. The agent screen pop should include a prompt to recite the announcement and seek the caller's OK to be recorded. If given, the agent should manually activate the recorder and record the caller's permission.
- When receiving calls from two or multi-party consent states, it is advisable to record the announcement as well as the call.
- Always secure in writing the agent's agreement to be recorded.
- When placing outbound telemarketing calls to two-party consent states, it is advisable to override the automatic announcement and require agents to manually recite the announcement and then activate the recorder, as appropriate. It is not good salesmanship to begin a telemarketing call with "This call may be recorded…"

Telemarketing Sales Rule

- Except as noted above, outbound telesales organizations should record a high percentage of interactions and spot check frequently for compliance.
- Agents should be trained on how to flag any interactions that involve express verifiable authorization. These calls should all be recorded and indexed and archived separately.
- Scripts should be prepared and followed that include all mandatory disclosures.
- Quality evaluations should consider the clarity, precision, and completeness with which mandatory information is disclosed. The script for oral authorizations must include the seven required pieces of information.

- Primarily inbound contact centers that encourage service-oriented agents to secure revenue growth must comply with TSR just as outbound telesales firms. In the event an inbound call is converted to a new sale, up-sell or cross-sell the agent needs to be trained to initiate recording and prompted to provide all required disclosures.
- In the event the original agent needs to transfer the call to a different individual to execute the sale the second agent must be trained to announce the company he/she represents.
- The recording technology deployed should have a thorough indexing mechanism that allows management to quickly and easily retrieve recorded transactions by several variables. At a minimum, the recordings should be retrievable-by date, time, agent, product or service, and any available customer identification information.
- If the selling organization already has pre-acquired account information, such as credit or debit card numbers, the agent must secure confirmation by asking the buyer for the last four digits of their credit or debit card. **All transactions of this type must be recorded and separately maintained.** It is good security practice for the agent **not to** have visual access to the entire card number – just the last four digits.

Truth-in-Lending Act

- Agents promoting the issuance of credit cards and other credit facilities must be trained on mandatory disclosures. A script should be prompted to help assure compliance. These calls should all be recorded and separately archived.

Fair Debt Collection Practices Act

- All collection calls by third-party collectors, whether to one-party or two-party consent states, **should be recorded**.
- It is advisable to announce a voice recording is being made, whether or not it is legally required. The simple process of hearing that the call may be recorded will encourage more forthright responses from the debtor.
- It is advisable to record a sampling of debt collection calls to persons other than the debtor for the purposes of acquiring information. This information will be a part of the quality assessment process, specifically to help assure that the collector properly identified him/herself and did not make any statements or allegations about the debtor.
- The quality evaluation process should carefully examine recorded collection calls to assure that the agent has not made any false representations, used harassing or intimidating language, or made any factual errors.
- Collection firms should consider investing in speech analytics software to quickly isolate potential violations.

Verification

- Verification and liability-conscious businesses are extending recording capability to business functions beyond the contact center. Examples may include purchasing, credit and collections, and investor relations. For calls to or from parties located in two-party consent states an announcement that the call will be recorded is mandatory.
- From a business etiquette standpoint it may be advisable to let the distant party know he/she is being recorded, even if such notice is not legally required.
- Rule 34 of the Federal Rules of Civil Procedure defines electronically stored information (ESI). Electronic information may be requested by parties to a legal dispute. Voice mail and other methods of recording spoken dialogue are subject to legal discovery. Voice mail systems typically allow recording of live calls, but it can be difficult and costly to retrieve these calls. Extending call center-recording to other functions makes it much easier to archive and retrieve requested voice interactions.

Consumer data security

- It is sound practice to prevent call center agents from recording or visually accessing sensitive consumer information such as credit cards, social security cards, and medical information. There is technology available today that masks sensitive information from computer screens and prevents recording of complete card numbers.

Health Insurance Portability and Accounting Act (HIPAA)

- The only practical and comprehensive way to determine compliance from telephone communications is to record all voice interactions then either spot check via quality monitoring to find any violations or use speech analytics to search the total archive for suspect words or phrases.
- Outsourcers and internal contact centers need to be very careful about the amount of information shared with agents. The fewer people that have access to PHI, the fewer the chances of disclosure. Collectors, for example, should have no reason to know the specific medical conditions that led to unpaid bills. CRM systems should be cleansed of PHI unless the information is deemed essential to providing services.

- Outbound callers, whether large contact centers, small doctor's offices, or local pharmacies, must be careful about the information they leave on patient answering machines and voice mail systems. These can be accessed by anyone. The Privacy Rule permits disclosure of limited information to family and others provided permission is granted.
- Agent evaluations should include scores on compliance.
- By law, a covered entity must train all workforce members on its privacy policies and procedures and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule. All health care contact center personnel should be trained on key provisions of the Privacy Rule.
- Outsourced contact centers and collections firms should include language in their agreements granting safe harbor in the event their clients practices are later found to be in violation of the Privacy Rule.

Sarbanes-Oxley

- Contact center agents should have access to corporate press releases at the same time they are released to the general public. If agents receive calls pertinent to the press releases, they should not disclose anything that is not in the release. Calls from the press or the investment community should be referred to the public relations or investor relations departments, as appropriate.
- Employees of large-cap publicly traded companies expect that the outside auditing firm will carefully review policies and practices within the contact center operation. Contact center management should work closely throughout the year with compliance officers and legal counsel to assure that operations are compliant with legislative mandates. It is not good practice to wait until the audit to get the proper paperwork and processes in place.
- Contact center managers have an obligation to inform other business functions of valuable technologies that could be put to use in other organizations. Contact centers in large public companies will already have an interaction recording system in place as well as a set of mature practices for extracting maximum value from the system. These can economically be extended to functions like investor relations and finance.

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 in-depth reports on interactive voice response, workforce management, performance management, and interactions recording. Dick's articles and observations have been published in CRM Today, Contact Center World, Customer Interaction Solutions, CRM Magazine, Call Center Magazine, Contact Professional, Call Center News, Speech Technology, Workforce Performance Solutions, and several other trade and business publications. 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 HIGHERGROUND

HigherGround, Inc. is a premier software developer of data collection and reporting tools coupled with call recording and quality assurance solutions for call centers and the public safety marketplace. The company's call recording, monitoring and reporting capabilities empower clients with knowledge and insight to monitor and verify phone and data transactions, optimize communications resources, and provide a comprehensive view of organizational performance. HigherGround's proven solutions provide imperative data for compliance monitoring, risk management, and performance improvement. More information regarding HigherGround can be obtained at www.highergroundinc.com.

CONTACT

HigherGround, Inc.
Robert Bowman, Senior Marketing Manager
818.456.1600 x 257
rbowman@higherground.com