



NAVIGATING THE
CHALLENGING
REGULATORY
LANDSCAPE
IN YOUR
CONTACT
CENTER



Contents

Introduction	3
Complex Contact Center Compliance	4
One Law to Rule Them All?	5
The Top Data Security & Compliance Regulations, Laws and Standards Bodies to Know	6
1. California Invasion of Privacy Act (CIPA)	7
2. Dodd-Frank Wall Street Reform and Consumer Protection Act	7
3. Do-Not-Call Implementation Act & the Telemarketing Sales Rule	7
4. Electronic Communications Privacy Act (ECPA)	8
5. Electronic Fund Transfer Act (EFTA)	8
6. Fair Debt Collection Practices Act (FDCPA)	8
7. Federal Deposit Insurance Corporation (FDIC)	9
8. Financial Conduct Authority (FCA)	9
9. Financial Industry Regulatory Authority (FINRA)	9
10. General Data Protection Regulation (GDPR)	10
11. Gramm-Leach-Bliley Act or Financial Services Modernization Act	10
12. Health Insurance Portability and Accountability Act (HIPPA)	10
13. Investment Industry Regulatory Organization of Canada (IIROC)	11
14. National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law	11
15. National Automated Clearing House Association (NACHA)	11
16. New York State Department of Financial Services (DFS) Cybersecurity Regulation	12
17. Payment Card Industry Data Security Standard (PCI DSS)	12
18. Personal Information Protection and Electronic Documents Act (PIPEDA)	12
19. Privacy Amendment (Notifiable Data Breaches) Act	13
20. Sarbanes-Oxley Act	13
21. Truth in Lending Act (TILA)	13
22. U.S. State Data Breach Notification Laws	14
How to Simplify Compliance	15
Conclusion	16



Introduction

As any CIO, CISO or security professional will attest, complying with today's ever-changing data security regulations is not easy. The time investment and complexity involved to ensure all the proper controls are in place are growing, as are the actual fines imposed on those who fail. For example, noncompliance with the Payment Card Industry Data Security Standard (PCI DSS) can result in fines anywhere between \$5,000 and \$500,000 a month*.

Failure to comply with today's most important regulations may also mean that your data security strategy is full of gaps, which put customers' personally identifiable information (PII) and your company's reputation at risk. With data breaches occurring at a record-breaking pace (in 2017, there were **1,579 data breach incidents** in the U.S. alone), there has never been a more crucial time to amplify your compliance efforts.

Consider the now-infamous Equifax breach, which exposed 147.9 million Americans' PII. It is believed to be the largest breach in history, costing Equifax more than **\$439 million** and leaving the company struggling to repair its reputation and make amends with customers. Undoubtedly, a single breach can be disastrous to your entire organization, your customers and your livelihood – which makes handling and storing “toxic” PII an outright liability.

* Source: <http://www.focusonpci.com/site/index.php/pci-101/pci-noncompliant-consequences.html>



Complex Contact Center Compliance

An overlooked area of your business that requires scrupulous attention to compliance is your contact center.

For enterprise contact centers, keeping up with the many different industry, country, regional and state regulations can be a huge burden, but vital to your company's overarching security strategy. Because contact centers collect, process and store vast amounts of PII – from credit card numbers and social security numbers (SSNs), to addresses and birthdates – they are prime targets for fraudsters and hackers.

Further complicating compliance for contact centers are the varying rules for handling call recordings and the data they contain. What PII is prohibited from being recorded or stored in those recordings? And, what happens when a contact center must also comply with regulations that require the recording of the entire call? For example, the PCI DSS bars the recording and storing of Sensitive Authentication Data (SAD) for credit and debit cards. Yet, in the U.S., the Electronic Funds Transfer Act (EFTA) requires the recording and retention of telephone conversations that authorize electronic funds transfers.

Such complexities lead contact centers to adopt “pause and resume” or “stop/start” solutions which allow agents and customer service representatives (CSRs) to pause a recording manually or automatically while PII, such as credit card numbers, is read aloud. The recording is resumed once the information is captured. However, this method creates further issues, as pause and resume systems are prone to failure due to simple human error. For instance, an agent may forget to pause the recording, inadvertently capturing PII on a recording that may be breached. On the other hand, a CSR could forget to resume the recording, leaving out much of the information required to comply with regulations like the EFTA.



One Law to Rule Them All?

Despite the rise in data breaches, there is still no single, all-encompassing global data security regulation... yet.

The European Union (EU) General Data Protection Regulation (GDPR), enacted in May 2018, regulates how businesses must treat sensitive data pertaining to EU citizens, regardless of where that business operates. Because it affects even businesses outside the EU, it is the closest we see to a global data security legislation at this point. Even so, it wasn't until 2017 that the first U.S. state introduced its own cybersecurity law – the New York State Department of Financial Services (DFS) Cybersecurity Regulation.

While we will likely see more countries follow in the EU's footsteps – such as Australia, which enacted its Notifiable Data Breaches (NDB) scheme in February 2018 – we are still years away from a truly global mandate. In the meantime, the world will have to adhere to a patchwork of different regulations.

Just as there is no all-inclusive, global data protection mandate, there is no solution for complying with each and every regulation. However, this guide will provide a few tactics to help enterprise contact centers dramatically simplify the process.

But first, let's take a closer look at some of the most prominent industry, country and regional regulations, laws and standards bodies that could impact today's contact centers.



The Top Data Security & Compliance Regulations, Laws and Standards Bodies to Know

1

California Invasion of Privacy Act (CIPA)

Type: U.S. State

Geographic Impact: U.S.

Overview: California enacted Penal Code Section 632, which requires all-party consent for recording confidential communications. Therefore, all inbound and outbound calls should be prepended with an announcement: “This call may be recorded for quality-assurance and training purposes.”

Who Must Comply: Any organization that conducts business with California residents via telephone.

What is in Scope: PII captured without all party consent.

2

Dodd-Frank Wall Street Reform and Consumer Protection Act

Type: U.S. Federal

Geographic Impact: U.S.

Overview: Also known as the Dodd-Frank Act, this legislation was designed to promote the financial stability of the U.S. markets by improving accountability and transparency in the financial system. The legislation outlines the requirement to record all oral communications relating to pre-execution swap trade information, including communications that ultimately lead to a related cash or forward transaction. Additionally, financial organizations are required to maintain all such records in a manner that is searchable by transaction and counterparty for up to five years.

Who Must Comply: Financial institutions.

What is in Scope: Trade information, call recordings.

3

Do-Not-Call Implementation Act & the Telemarketing Sales Rule

Type: U.S. Federal

Geographic Impact: U.S.

Overview: To reduce the volume of telemarketing calls consumers receive, Congress passed the Do-Not-Call Implementation Act. Telemarketers who make sales and take orders are required to obtain a customer’s direct and verifiable authorization when they agree to be billed. They must also identify the method of payment, including a statement that the customer understands he or she will be billed, and the specific amount and date on which the charge will be submitted. 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.

Who Must Comply: All industries.

What is in Scope: Call recordings and transaction evidence.

4

Electronic Communications Privacy Act (ECPA)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Electronic Communications Privacy Act (sometimes called the Wiretap Act) protects the privacy of wire, oral and electronic communications while those communications are being made, are in transit or when they are stored on computers. The act applies to telephone conversations, email and data stored electronically. It protects the privacy of such communications and prohibits the interception, attempted interception, use, disclosure or procurement of these communications. It also prohibits the use of illegally obtained communications as evidence in a court of law. Individuals who violate ECPA face up to five years in prison and fines up to \$250,000. Victims are also entitled to bring civil suits and recover actual damages, in addition to punitive damages and attorney fees.

Who Must Comply: All U.S. organizations and individuals.

What is In Scope: Wire, oral and electronic communications while they are being made, are in transit or stored on computers. This applies to telephone conversations, email and data.

5

Electronic Fund Transfer Act (EFTA)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Electronic Fund Transfer Act (EFTA) is a federal law enacted in 1978 to protect consumers when they use electronic means to manage their finances. Electronic fund transfers are defined as transactions that use computers, phones or magnetic strips to authorize a financial institution to credit or debit a customer's account. The EFTA requires recording and retention of telephone conversations that authorize electronic funds transfers.

Who Must Comply: U.S. financial institutions and any third party involved in EFT services.

What is in Scope: Call recordings.

6

Fair Debt Collection Practices Act (FDCPA)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Fair Debt Collection Practices Act (FDCPA) prohibits conduct by debt collectors that could be considered abusive or deceptive. This includes restrictions on when consumers can be contacted by telephone, misrepresentation of the debt or the debt collector's legal authority. Maintaining full call recordings protects agencies against FDCPA claims. But, without the full valid recording of the call it may be difficult for debt collectors to clear themselves of wrongdoing. Call recordings are typically digitally "watermarked" to prevent tampering – which is difficult to implement and maintain if the recording has been broken into multiple files or is silent during important transactional stages.

Who Must Comply: Debt collection agencies.

What is in Scope: Debt collection practices, call recordings.

7

Federal Deposit Insurance Corporation (FDIC)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Federal Deposit Insurance Corporation (FDIC) preserves and promotes public confidence in the U.S. financial system by insuring depositors for at least \$250,000 per insured bank. This is done by identifying, monitoring and addressing risks to the deposit insurance funds; and by limiting the effect on the economy and the financial system when a bank or thrift institution fails. Among other things, the FDIC regulates the recording of telephone call details at financial institutions. FDIC 30-64-0020 Telephone Call Detail Records states that calls can be full or partial; however, they need to be password protected and accessible only by authorized personnel. This rule states: "Records are destroyed after the close of the fiscal year in which they are audited or after three years from the date the record was created, whichever occurs first." However, depending on the nature of the call contents this can change drastically:

- FDIC-30-64-0022 for Freedom of Information Act and Privacy Act requests requires that electronic call records are stored for five years.
- FDIC-30-64-0025 for Beneficial Ownership Filings requires that calls "will be maintained for 15 years from the date of filing."

Who Must Comply: Financial institutions in the U.S.

What is in Scope: PII and call recordings.

8

Financial Conduct Authority (FCA)

Type: U.K. Industry

Geographic Impact: U.K.

Overview: The Financial Conduct Authority (FCA) is a financial regulatory body in the United Kingdom, but operates independently of the U.K. government, and is financed by charging fees to members of the financial services industry. The FCA regulates financial firms providing services to consumers. It focuses on the regulation of conduct by both retail and wholesale financial services firms and its mission is to implement, supervise and enforce the EU and international standards and regulations in the U.K. The FCA has significant authority, including the power to regulate conduct related to the marketing of financial products, as well as to place minimum standards and requirements on financial products. It is also the authority responsible for regulating the consumer credit industry in the U.K. In 2015, the FCA created a separate entity, the Payment Systems Regulator (PSR), which is tasked with promoting competition and innovation in payment systems, and ensuring they work in the interests of the organizations and people that use them.

Who Must Comply: The FCA has the power to investigate organizations and individuals in the U.K. It regulates banks, mutual societies and financial advisers in order to protect consumers and promote fair competition.

What is in Scope: Financial products sold or marketed to U.K. citizens.

9

Financial Industry Regulatory Authority (FINRA)

Type: U.S. Industry

Geographic Impact: U.S.

Overview: The Financial Industry Regulatory Authority, Inc. (FINRA) is a private corporation that acts as a self-regulatory organization (SRO). It is a non-governmental organization that regulates member brokerage firms, exchange markets and the arbitration operations of the New York Stock Exchange. The government agency that acts as the ultimate regulator of the securities industry, including FINRA, is the Securities and Exchange Commission. In 2014, FINRA adopted Rule 3170 – Tape Recording of Registered Persons by Certain Firms, commonly referred to as the "Taping Rule." It establishes and enforces special supervisory procedures, including the tape recording of conversations, for certain broker/dealer firms when they have hired more than a specified percentage of registered persons from firms that have been expelled or that have had their broker/dealer registrations revoked for violations of sales practice rules ("disciplined firms").

Who Must Comply: Brokerage firms that have been expelled or had their broker/dealer registrations revoked for violations of sales practice rules.

What is in Scope: Taped recordings of telephone and oral conversations between brokers and their clients.

10

General Data Protection Regulation (GDPR)

Type: European Union (EU) regulation

Geographic Impact: Global – any firm that collects, processes or stores sensitive PII on EU residents must comply, whether or not that firm operates in the EU.

Overview: The GDPR is an EU regulation intended to strengthen and unify the protection of personal data for all EU citizens. It applies to all EU companies, as well as foreign companies that process or store PII on EU residents. The GDPR establishes strict requirements for obtaining consent when collecting data; the need to alert the relevant supervisory authority of data breaches within 72 hours of occurrence; and the “right to be forgotten,” in which data subjects can request the deletion of personal information that is no longer serving its original purpose. Non-compliant organizations can be fined up to €20 million or four percent of annual revenue, whichever is greater.

Who Must Comply: Any organization that collects data from EU residents (i.e. a data controller) or processes or stores data on behalf of a data controller (e.g. cloud service providers) when the data subject (person) is based in the EU. The regulation applies to organizations based within the EU as well as those outside the EU that collect, process or store data on EU residents.

What is in Scope: PII relating to any EU resident, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information or a computer’s IP address.

11

Gramm-Leach-Bliley Act or Financial Services Modernization Act

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Gramm-Leach-Bliley Act requires financial institutions to explain their information-sharing practices to their customers and give customers the right to “opt-out” if they don’t want their information shared with certain third parties. The Safeguard Rule in the law also requires financial institutions to protect sensitive consumer information. It states that financial institutions must create and follow a written information security plan that details how they will protect their current and legacy customers’ non-public information, such as account and identification numbers. Call recordings, therefore, provide evidence that an institution is actively practicing compliance with GLBA. Calls with broken recordings do not provide the same levels of auditability.

Who Must Comply: The law applies not only to financial institutions, but also to many businesses that may not normally consider themselves a financial institution. In fact, the Safeguard Rule applies to all businesses, regardless of size, that are “significantly engaged” in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguard Rule also applies to companies like credit reporting agencies and ATM operators that receive information about the customers of other financial institutions.

What is in Scope: Any type of sensitive PII. This can include names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and social security numbers.

12

Health Insurance Portability and Accountability Act (HIPAA)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: Established under the Security Standards for the Protection of Electronic Protected Health Information (the Privacy Rule), HIPAA provides data privacy and security provisions for safeguarding medical information that is held or transferred in electronic form. The goal of the regulation is to protect the privacy of individuals’ health data, while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. HIPAA’s fundamental requirement for covered entities and their business associates is that Protected Health Information (PHI) must be secured.

Who Must Comply: Covered entities – health plans, healthcare clearinghouses, healthcare providers and business associates who electronically transmit any health information.

What is in Scope: Protected Health Information (PHI).

13

Investment Industry Regulatory Organization of Canada (IIROC)

Type: Canadian Industry

Geographic Impact: Canada

Overview: A self-regulatory organization that oversees all investment adviser firms in Canada, IIROC sets regulatory and investment industry standards, protects investors and strengthens market integrity while maintaining efficient and competitive capital markets. Trading activity is monitored through the Surveillance and Trading Review and Analysis departments – monitoring dealers, their employees and trading activity. The self-regulatory process must include a commitment to transparency, disclosure, fairness and accountability. If monitoring efforts or preliminary investigations detect evidence of possible insider trading activity, a violation of provincial securities acts, the details are referred on to the appropriate provincial regulator – as IIROC records all calls to and from Market Surveillance team telephone lines.

Who Must Comply: IIROC's regulated dealer firms and their registered employees with rules related to business conduct, financial operations and trading practices.

What is in Scope: Call recordings.

14

National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law

Type: U.S. Industry

Geographic Impact: U.S. and five U.S. territories.

Overview: NAIC is a non-governmental standard-setting and regulatory support organization created and governed by chief insurance regulators from the U.S. and five U.S. territories. The NAIC's Insurance Data Security Model Law provides rules for insurers, agents and other licensed entities covering data security and breach investigation and notification. Requirements include maintaining an information security program based on ongoing risk assessment, overseeing third-party service providers, investigating data breaches and notifying regulators of a cybersecurity incident.

Who Must Comply: Insurers, agents and other licensed entities.

What is in Scope: Non-public information (NPI).

15

National Automated Clearing House Association (NACHA)

Type: U.S. Industry

Geographic Impact: U.S.

Overview: The National Automated Clearing House Association (NACHA) is a non-profit membership association that oversees the Automated Clearing House (ACH) system, which operates the largest electronic payment network in the world. Rules apply to any business that processes ACH transactions using a system that creates "entries" into the ACH network, either by converting a paper check document into an ACH transaction or by entering a customer's bank account information to process a direct payment or direct deposit transaction. As a result, contact centers that record calls must secure or redact all protected financial information.

Who Must Comply: Any organization that processes bank payments and ACH transactions.

What is in Scope: Financial information, sensitive non-financial information and PII, and call recordings.

16

New York State Department of Financial Services (DFS) Cybersecurity Regulation

Type: U.S. State

Geographic Impact: State of New York/any entity conducting business in New York

Overview: The first cybersecurity regulation in the U.S., this mandate aims to protect New York consumers and financial institutions from the ever-growing threat of cyberattacks. The regulation requires banks, insurance companies and other financial services institutions it regulates to establish and maintain a cybersecurity program. They must also encrypt non-public information (NPI) – such as payment card numbers, social security numbers, driver's license numbers and other security codes, both in-transit and at-rest.

Who Must Comply: Financial services companies that conduct business in the state of New York.

What is in Scope: Non-public information (NPI) and call recordings.

17

Payment Card Industry Data Security Standard (PCI DSS)

Type: Industry Standard

Geographic Impact: Global

Overview: Established by the Payment Card Industry Security Standards Council (PCI SSC), the PCI DSS is a set of requirements for securing payment transactions and protecting cardholders against misuse of their personal information. Although the PCI SSC defines multiple levels of merchants and service providers, the requirements remain the same for all entities. In addition to the 12 high-level requirements the PCI SSC outlines in the DSS, there are numerous sub-requirements, and potentially hundreds of controls – making the PCI DSS one of the most complex, industry-wide regulations. Notably, payment card data that is stored in call recordings is in scope for compliance, while the PCI DSS explicitly prohibits storing Sensitive Authentication Data (SAD) like CVVs.

Who Must Comply: Any organization that processes, stores or transmits payment card data.

What is in Scope: Cardholder data, including PAN (Primary Account Numbers), SAD (CVV/C/2), Magnetic Stripe, from the major card schemes.

18

Personal Information Protection and Electronic Documents Act (PIPEDA)

Type: Canadian Federal

Geographic Impact: Canada

Overview: Enacted as a Canadian federal privacy law for private-sector organizations, PIPEDA establishes a right to the protection of personal information collected, used or disclosed in the course of commercial activities, federal contracts or commerce between provinces or internationally. It imposes the following principles on data gatherers: encouraging accountability; identifying the purposes for the collection of personal data; obtaining consent; limiting collection; limiting use and disclosure of data; ensuring accuracy; providing adequate security; announcing information management policies; and providing individuals a right to access information about themselves, and a right to challenge an organization's compliance with these principles. Specifically, PIPEDA requires businesses to use the appropriate security safeguard to protect personal information, such as passwords, encryption and firewalls for electronic data.

Who Must Comply: Canadian federal works, undertakings or businesses (FWUBs).

What is in Scope: Personal information, electronic documents, electronic signatures.

19

Privacy Amendment (Notifiable Data Breaches) Act

Type: Australian Government

Geographic Impact: Australia

Overview: The passage of the Privacy Amendment (Notifiable Data Breaches) Act in 2017 established the Notifiable Data Breaches (NDB) scheme in Australia. The NDB scheme applies to all agencies and organizations with existing personal information security obligations under the Australian Privacy Act. The NDB scheme introduced an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. This notification must include recommendations about the steps individuals should take in response to the breach. In addition, the Australian Information Commissioner must be notified of eligible data breaches.

Who Must Comply: Australian government agencies, businesses and not-for-profit organizations with an annual turnover of \$3 million or more, credit reporting bodies, health service providers, and TFN recipients, among others.

What is in Scope: PII, which if breached, would likely result in “serious harm” to any individual affected.

20

Sarbanes-Oxley Act

Type: U.S. Federal

Geographic Impact: U.S.

Overview: Enacted in 2002 in response to public accounting malpractices involving major businesses, the Sarbanes-Oxley Act (SOX) aims to protect investors from the possibility of fraudulent accounting activities by corporations. SOX mandates that businesses create and maintain electronic records as part of their regular business processes. In doing so, all financial reports must include an Internal Controls Report, while log collection and monitoring systems must provide an audit trail of all access to and activity surrounding sensitive business information. Therefore, it is important that any business conducting transactions over the phone has a complete record of that transaction to better adhere to SOX and the audit processes it requires.

Who Must Comply: All private and publicly held companies in the U.S.

What is in Scope: Business processes and transactions.

21

Truth in Lending Act (TILA)

Type: U.S. Federal

Geographic Impact: U.S.

Overview: The Truth in Lending Act (TILA) intends to protect consumers against inaccurate and unfair credit billing and credit card practices by requiring complete and meaningful disclosure of all credit terms in simple, easy-to-read language. Contact centers that are involved in home mortgages, credit card 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. It is therefore a best practice to record all call and screen recordings.

Who Must Comply: Consumer lending institutions including banks, credit unions and finance companies.

What is in Scope: Credit card transactions and billing, call recordings.

U.S. State Data Breach Notification Laws

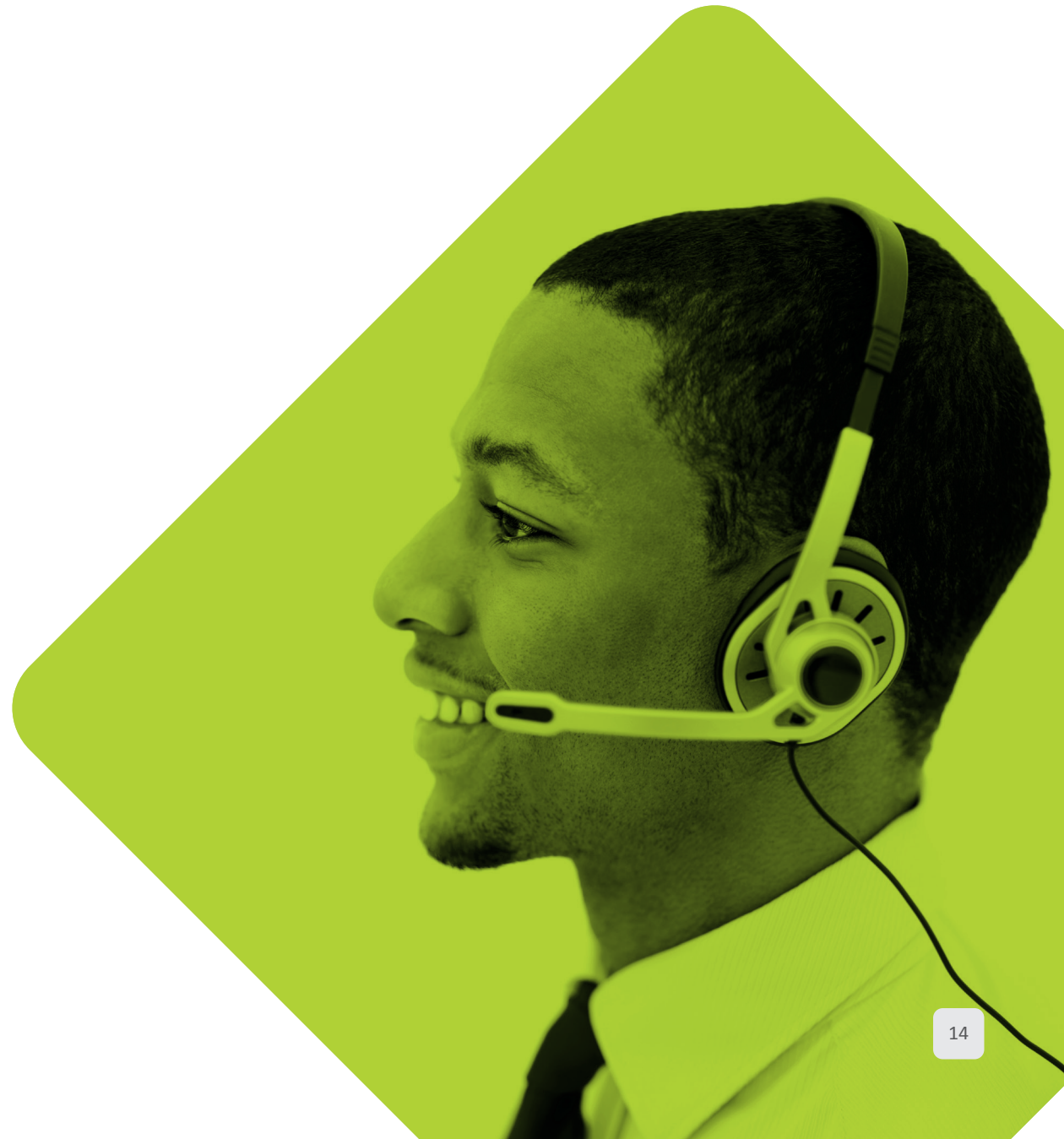
Type: U.S. State

Geographic Impact: Individual U.S. States

Overview: All 50 U.S. states, along with the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have some form of legislation that requires private or government entities to notify individuals of security breaches of information involving PII. While the specifics vary from state to state, the goal is the same: to protect businesses and consumers alike from the adverse impacts of data breaches. For example, the Massachusetts Data Breach Notification Law – believed to be one of the strictest in the U.S.– requires businesses and others that own or license personal information of residents of Massachusetts to notify the Office of Consumer Affairs and Business Regulation and the Office of Attorney General when they know or have reason to know of a security breach. They must also provide notice if they know or have reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person or used for an unauthorized purpose. In addition to providing notice to government agencies, businesses must also notify the person(s) whose information is at risk.

Who Must Comply: Businesses and other organizations that own or license personal information of residents of individual U.S. states.

What is in Scope: PII.





How to Simplify Compliance

While this list is only a snapshot of some of today's most prominent data protection laws, it shows how complex the regulatory landscape has become.

So, how can you streamline contact center compliance? Instead of struggling to determine which regulations apply and when, what controls you must have in place and how a violation may impact your organization, you can dramatically simplify compliance by treating all PII as "toxic." This means removing as much sensitive data as possible from your business IT infrastructures. For numerical data, such as credit card, social security and bank account numbers, this is easily achievable with dual-tone multi-frequency (DTMF) masking technologies.

DTMF masking technologies allow callers to enter numerical PII directly into their telephone keypad. The keypad (DTMF) tones are masked with flat tones so that agents, CSRs and even eavesdroppers are not exposed to the sensitive data, nor is data captured on call recording systems. This eliminates the need for unreliable pause and resume solutions and allows contact centers to record full conversations when needed.

In addition, DTMF masking solutions – unlike interactive voice response (IVR) systems – allow agents to remain in full voice communication with callers throughout the transaction, ensuring a positive customer experience. Once PII is captured, it is sent directly to the appropriate third party (such as a payment processor), bypassing the contact center's network completely.

As a result, the entire contact center remains out of the scope of compliance for the PCI DSS and many other regulations. More importantly, PII no longer resides in desktop applications and call recording systems where it is vulnerable in the event of a breach.



Conclusion

As data breaches continue to occur at an alarming rate, the regulatory compliance landscape will further evolve to protect consumers and safeguard the increasing amount of information shared in today's digital age. However, it is important to understand that compliance does not equal security: an organization is not necessarily secure just because it is compliant. Rather, it is the other way around: an organization is compliant because it is secure. Hackers and fraudsters every day are finding new ways to tap into your organization's sensitive data and expose its vulnerabilities. Therefore, companies should look for ways to go above and beyond compliance requirements.

To secure your customers' most sensitive data – and therefore, secure your company's reputation – start with your contact center. There, you can best prepare for the regulations of today and tomorrow by removing as much toxic PII from their environment as possible.

After all...


**They can't hack the data
you don't hold.**



About Semafone

Semafone provides data security and compliance solutions for contact centers. Since our inception in 2009, we've watched closely as the regulatory landscape has evolved to strengthen data protection and privacy across industries around the world. In doing so, we deliver software that descopes contact centers and their business IT environments completely from the PCI DSS, and simplifies compliance with many other complex regulations. Our flagship solution Cardprotect ensures customer credit card numbers never touch the contact center's infrastructure, desktop applications and CRM systems, and prevents exposure to agents and call recording systems by using DTMF masking technology. The results? Compliance is dramatically simplified, data is safe, businesses' reputations are intact and customers are happy.



 +1 888-736-2366

 info@semafone.com

 www.semafone.com

 @semafone

 LinkedIn

 745 Atlantic Ave. Boston, MA 02111

