WHITE PAPER

Compliance Adherence Made Simple With Acqueon Engagement

As the world steadily moves digital, information security compliance is taking increasingly paramount significance within organizations, and as a result, regulations are becoming stricter than ever! A lot of these data regulations today fall within the scope of contact centers that receive, process, and store a range of Personally Identifiable Information (PII), such as addresses, telephone numbers, dates of birth, card numbers, account numbers, social security numbers, and more. It requires that contact centers make compliance their absolute top priority.

In 2012, one of the largest banks in the United States, Capital One, entered into a legal hazard by referring credit card customers with low credit scores to third-party vendors that operated call centers, pitching credit card add-on products such as payment protection plans and credit monitoring services. The vendors used high-pressure sales tactics and misleading practices to sign customers up, and Capital One failed to monitor them. As a result, Capital One agreed to pay $210 million in fines and penalties in a settlement reached with federal banking and consumer protection regulators.

In 2013, the Federal Trade Commission (FTC) held Mortgage Investors Corporation, one of the leading mortgage lenders in the US, to account for violating the Do Not Call provisions of the Telemarketing Sales Rule (TSR) of the agency. The company paid a civil penalty of $7.5 million, the biggest fine ever collected by the FTC. During telemarketing calls, the company failed to remove consumers from its DNC lists on-demand and misrepresented the terms of available loan products.

In the following year, the Consumer Financial Protection Bureau (CFPB) ordered another banking giant Synchrony Bank, previously known as GE Capital Retail Bank (GE Capital), to pay a whopping $225 million in relief to the consumers who were harmed by illegal and discriminatory credit card practices. The Bureau found that GE Capital's telemarketers had misinterpreted the add-on products and had not disclosed that certain classes of consumers were not eligible for these products.

These examples indicate the risks and the impact of the regulations on contact centers. Now, let's look at some of the top data privacy and security regulations governing contact centers across industries like banking, insurance, credit cards, healthcare, telecom, etc.

Contact centers are at the front line of customer service, but regulations can sometimes stand in the way, adding a new layer of complexity in operations and campaign management.

Data Privacy and Security Regulations Impacting Contact Centers

1. Consent to Record

There are several federal and state wiretapping laws that limit the ability of contact centers to record phone calls or conversations in-person. From a regulation point of view, the most critical aspect is that one should obtain the consent of one or all of the parties to a phone call or conversation before recording it. Federal law and many state wiretapping statutes allow recording if one party consents to a phone call or chat. Other states, on the other hand, require the consent of all parties to the communication.

Violations may result in imprisonment of no more than five years, and fines of up to **$500,000 for organizations.**

2. Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is an information security standard designed to ensure the security of credit, debit, and cash card transactions and to protect cardholders from misuse of their personal information. Created jointly in 2004 by four major credit card companies: Visa, MasterCard, Discover and American Express, it sets out six main objectives such as network security, protection of cardholder information, system protection against hackers, viruses, spyware and malware programs, restriction and control of access to system information and operations, security measures for network monitoring, and

implementation of formal information security policies. **The consequences of not being compliant with PCI range from $5,000 to $500,000.**

3. General Data Protection Regulation (GDPR)

Designed to harmonize data privacy and security legislation across Europe, the EU General Data Protection Regulation (GDPR) mandates a base set of standards for all companies handling the personal data of EU citizens. Some of the critical privacy and data protection requirements of the GDPR include requiring the consent of data processors, anonymizing the data collected to protect privacy, providing notifications of infringements of data, safe handling of cross-border data transfers, and requiring individual companies to appoint a data protection officer to oversee compliance with the GDPR. **Penalties for violations of GDPR may result in a fine of up to EUR 20 million or up to 4% of the company's annual worldwide turnover.**

5. Markets in Financial Instruments Directive II (MiFID II)

MiFID II is a legislative framework established by the European Union to regulate and improve financial markets and protect investors. It aims to standardize practices across the EU and restore industry confidence, especially after the 2008 financial crisis. It covers virtually all institutional and retail investors, financial firms, and professionals within the EU, such as bankers, traders, fund managers, exchange officials, and brokers, all have to abide byits rules. Penalties are laid down by the regulatory agencies in each country. **The Financial Conduct Authority in the United Kingdom recently imposed a fine of £ 1.50 per line of incorrect or unreported data.**

4. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was designed to protect the data privacy and security of personal medical information. It includes regulations governing the use, storage, and access of "individually identifiable health information," i.e., past/present/future physical or mental health conditions, held or transmitted in any form or media, whether electronic, paper, or oral. HIPPA regulates healthcare providers and payors who maintain contact centers to handle member inquiries, provider inquiries, eligibility checks, care authorizations, and claims questions, among other types of calls. **Companies that violate HIPAA are subject to penalties by the U.S. Department of Health & Human Services.**

6. Telemarketing Sales Rule (TSR)

The TSR prohibits misleading and abusive telemarketing practices. TSR has established the National Do Not Call Registry, which makes it easier and more efficient to reduce the number of unnecessary telemarketing calls. The TSR sets standards of conduct for telemarketing calls, such as restricting telemarketers from calling customers before 8 AM and after 9 PM, identifying and

disclosing the vendor and the purpose of the call, etc. TSR prohibits telemarketers from lying about the terms of their offer. **Companies that violate the rules are subject to fines up to $11,000 per infringement.**

7. Telephone Consumer Protection Act (TCPA)

The TCPA regulates telemarketing calls and the use of automated telephone equipment. It limits the use of pre-recorded voice, automatic dialing, SMS, and fax messages without the express consent of the customer. Companies must abide by strict solicitation rules, and the National Do Not Call Registry, and the consumers may sue a company that does not follow the TCPA guidelines. Consumer consent is a crucial defense under the TCPA.

8. U.S. Electronic Funds Transfer Act (EFTA)

The EFTA is a federal law that protects consumers engaged in the transfer of funds by electronic means. It regulates contact centers for the use of electronic money transfers, debit cards,automated teller machines, and automatic withdrawals from bank accounts. The Act alsoprovides a means of rectifying transaction errors and limits the liability for any financial loss due to a lost or stolen card.

9. Fair Debt Collection Practice Act (FDCPA)

The FDCPA regulates third-party debt collectors who attempt to collect debts on behalf of another person or entity. It prohibits the use of threatening or abusive language and unfairor misleading practices in the collection of debts. Credit card debt, auto loans, medical bills, student loans, mortgages, and other household debts are covered by the FDCPA. No debt collector can contact the customer atinappropriate times or places without prior permission.

Some of these regulations complement one another, while others in some cases weaken or even contradict one another. For example, contact centers that accept telephone payments must comply with EFTA, which requires them to record telephone conversations that allow electronic fund transfer.

PCI-DSS, meanwhile, complicates this process by stipulating that certain information, such as CVV2 code, should never be recorded or stored. Many contact centers use "pause and resume" or "stop/start" call recording systems to try to comply with these different rules, which come with their problems.

In most U.S. states, when a call is monitored or recorded, the law requires at least one.

Companies that handle financial transactions have a responsibility to protect consumer data in the best possible way.

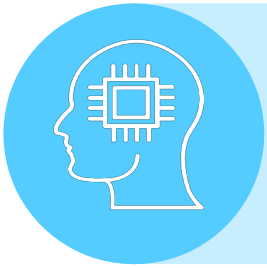
party to be notified, while a few other states and countries require all parties to be informed. Differences in these laws are difficult for contact centers to keep up with, especially when some states have regulations that are stricter than federal laws.

Staying on top of frequently changing/evolving regulations and making sure that your compliance programs are up to date is not easy. It requires overcoming the hectic process of sourcing, managing, and updating the federal Do-Not-Call data, portability details, and scouting for all litigators. **Here's where Acqueon comes in.**

Compliance Adherence Made Simple

Acqueon's AI-powered omnichannel, conversational engagement software is designed to automatically comply with the TCPA, DNC, and GDPR guidelines, integrated with its product features, and streamline the entire outbound campaign management at contact centers.

Its easy-to-use administration modules simplify the administrative and monitoring overheads by enabling administrators, supervisors, and campaign managers to configure rules and policies in real-time based on compliance checks. Acqueon's backend processing engine performs these compliance checks without affecting the performance of the contact center. **It enables companies to focus more on proactive customer engagement strategies and critical business objectives, without worrying much about statutory regulations and regional-specific regulatory adherence or soft compliance issues, which all impact customer satisfaction.**



Acqueon's AI-powered omnichannel, conversational engagement software is designed to automatically comply with the TCPA, DNC, and GDPR guidelines.

How Does Acqueon Simplify Compliance?

1. Acqueon's Partnership with DNC.com

Acqueon, through its partnership with DNC.com, combined with data processing modules optimized for large databases, provides easy access to federal Do-Not-Call lists on a very nominal annual subscription basis. Acqueon's efficient contact processing workflow simplifies the acquisition, processing, segmentation, and verification of their contact list against the federal DNC database.

In contrast to most dialers and list management systems on the market with complex customization to validate compliance with multiple data sources, which limits scrubbing activity only when data is uploaded during non-production hours,

Acqueon's platform comes with built-in data connectors that automatically refresh all data daily. This enrichment of the contact list prevents non-compliance by **proactively scanning all wireless numbers through a known litigator database as well as a master archive**.

2. Do Not Call Filtering

The platform also provides an option to filter through the DNC list and perform validation checks twice - at the time of contact upload and during each dial attempt. It gives the flexibility to do just-in-time validation before

dialing a contact during each attempt, apart from initial screening at the time of uploading. It enables the platform to auto-remove contacts from call lists if they appear on the Do Not Call List. Additionally, it supports filtering through corporate and campaign-specific DNC collections. Multiple utilities are provided to manage the DNC list at three levels — Federal, Enterprise, and Campaign levels. The APIs are available to add telephone numbers to the DNC list on an ad-hoc basis or in batch mode. Acqueon has the option to block any unique ID at the caller level.

3. Time Zone Compliance

The platform can identify the customer's time zone, either based on pre-determined business segmentation, zip code, or phone number area code, and ensures that contacts are reached within a reasonably accepted local time range.

Compliance features, specific to time zone identification, can map contact with multiple zip codes and identify a callable window that intersects with any time zone associated with these zip codes. This feature mainly complements two types of campaigns:

- Those involving a home mortgage or
- Campaigns involving a single call record containing multiple client phone numbers in different modes. In the case of no answer, these are to be reached sequentially based on a joint account relationship with the company.

These features are critical when a contact, associated with an account, resides in different time zones or, in the event of a primary asset being mortgaged, belongs to a time zone other than the person being contacted. These insights can be identified by associating time zones based on the zip code mapped to the asset, the primary account holder, and the secondary/third account holders, respectively, while uploading their contact numbers.

The system allows a maximum of two zip codes linked to the record level and one zip code for each contact phone number uploaded to the call level. The system dials these numbers at a mutually intersecting time interval across all mapped zip codes at the record level and the phone number that is being called. It ensures that customers are not distracted at odd times.

4. Silent and Abandoned Call Handling

Technically, on the platform, the call is disconnected either without a message being played (silent) or after a message has been played (abandoned). In both cases, the platform labels it as an abandoned call. The platform can be configured on how to handle an abandoned call, in the event of an agent not being available, either by rescheduling the contacts or by chaining them to a preview campaign depending on the availability of the agent.

5. Soft Compliance

Soft compliance is a crucial component, as it ensures that customers are not reached too many times during the campaign. It limits the number of attempts to a defined duration while percolating through the contacts in the lists. Acqueon can constrain/restrict the number of attempts over a specified duration; yet, at the same time, it percolates through all contacts in the uploaded lead list with the privacy instructions of the caller by not trying to annoy them with too many attempts.

6. Time of Day Misuse

The platform can configure permissible callable windows, allowing the agents to dial only within the scheduled time limits. It can also manage daylight savings to adjust the callable window.

7. Repeated Calling

The platform can control the number of attempts to call a number. The dialing restriction can be configured for a single day or several days to ensure that customers are not repeatedly disturbed over a reasonable period.

8. Ring Duration

The length of the ring can be configured by Acqueon. The minimum duration of the ring is 15 seconds, as standardized by OFCOM. The duration of the ring should not be extended for a longer period, as it may upset customers.

9. Record Management

Acqueon maintains a detailed record of calls made by dialer, IVR, or abandoned due to the non-availability of agents. It also captures the number of contacts, attempts, and outcomes. Custom reports can be built to comply with OFCOM.

10. Misuse for Dishonest Gain and CLI Facility

The platform can set or change the CLI while dialing a call. This feature is provided with the intention of either enabling the recipient to quickly identify the call or route the call to the relevant group if they choose to call back. The platform allows the inclusion of a prefix/postfix on a call numberso that the dialer can select the least call routing pattern or spoof CLI through which a customer can easily identify the caller or route the call back to the right agent group.

Acqueon's product features and compliance work hand-in-hand to provide a successful proactive customer engagement for contact centers.

11. The Two-Second Rule

The Two-Second Rule is a dialer functionality that is being configured on the dialer level. To improve the connect rate, the answer machine detection (AMD) or post-connect analysis can be switched off. In the event of a call drop, the solution ensures that the correct message is played within 2 seconds on call connect to specify on whose behalf the call was made and a brief note on the reason for the call.

12. The 24-Hour Rule

For AMD and abandoned calls, Acqueon can set the callback time to 24 and 72 hours, respectively. The Chaining feature moves a record from a Predictive Campaign to a Preview Campaign to ensure agent availability/reservation if a business needs to call within 72 hours. If the system uses AMD and detects that a call has been answered by the answering machine and the call is automatically terminated; as a result, the number cannot be retrieved for another 24 hours. Similar to the 72-hour rule, this rule can be ignored if a live operator is guaranteed to be available for further calls within 24 hours.

13. Screening TPS Data

The platform is capable of scheduling data refresh against the TPS/DNC list not only at the time of upload but also at each time. It ensures that TPS data is synchronized with the TPS/DNC data service provider at least once a week. Acqueon also provides the option to configure a specific TPS/DNC campaign list. The API is available to set those preferences for a campaign in real-time. The option of providing a time-bound do-not-call option is also available on the platform to customers who wish to suspend calls for a specific period for reasonssuch as being away from their home network,going on holidays, and not wanting to be distracted, etc.

To sum up, **Acqueon's product features and compliance work hand-in-hand to provide a successful proactive customer engagement for contact centers.** Our compliance strategy binds customer trust to data protection in a single effort. Acqueon's holistic compliance solution automates and simplifies the day-to-day compliance activities of all contact centers, bringing together assurance, analytics, and real-time actionable insights dedicated to compliance.

See How Acqueon Can Automate & Simplify Compliance for You:

marketing@acqueon.com | www.acqueon.com