Data privacy and security are critical concerns for organizations of all sizes and industries, but even more so for enterprise companies. In the era of digital transformation, businesses increasingly rely on contact centers to handle customer interactions on many channels. However, with the increase in cyberattacks and data breaches, there’s never been a more prudent time for highly secure and compliant contact center technology that protects sensitive information and meets regulatory requirements. This white paper will discuss why security and compliance matter in the contact center and what to look for when selecting secure and compliant contact center technology.

Why Contact Center Security Matters

Contact centers are hubs for sensitive information, including customer data, payment details, and personal identification information (PII). If this information is compromised, it can lead to significant financial and reputational damage for organizations. The need for contact center security is further amplified by data protection regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

A breach of customer data can lead to lawsuits, fines, and loss of customer trust, all of which can have long-term effects on a company’s bottom line. In fact, according to a recent report by IBM, the global average cost of a data breach in 2023 was USD 4.45 million, which is a 15% increase over three years. This means that the security of contact center technology is a critical concern that cannot be overlooked.

Why Contact Center Compliance Matters

In addition to security, contact center technology must meet regulatory requirements and should aim to have compliant-related functionality built into the technology itself. Compliance regulations are in place to ensure that companies protect customer data and maintain data privacy. Building compliant-related functionality right into the technology also makes it easy to abide by even the strictest compliance regulations. This is important, since failing to meet compliance requirements can result in significant penalties and fines. As we’re seeing from a recent CFPB report, consumer relief from compliance violations is continuing to increase. This resulted in USD $2.4 million in total consumer relief in 2022.

The Payment Card Industry Data Security Standard (PCI DSS) is a specific example of a compliance framework that applies to contact centers that handle credit card payments. PCI DSS sets security standards for protecting cardholder data during transactions. Failure to comply with PCI DSS can result in hefty fines and damage to an organization’s reputation. In fact, as of 2023, the baseline PCI
noncompliance penalties start at charges of $5,000 to $10,000 per month for the first three months of noncompliance, with charges increasing to up to $100,000 per month after the seventh month of noncompliance.

Especially when conducting proactive outreach to customers, there are also risks in terms of violating multiple laws and regulations. Some of the most well-known compliance regulations and laws are Do Not Contact (DNC) regulations, STIR/SHAKEN compliance, Ofcom, the Telephone Consumer Protection Act of 1991 (TCPA), the Fair Debt Collection Act (FDCS), and more. To make things even more complicated, many states and even specific jurisdictions have their own regulations and compliance laws to uphold. Without the proper technology with built in compliance-ready tools, it’s easy to violate these strict regulations and suffer financial penalties as a result.

Choosing the Right Contact Center Technology

Knowing the potential risks to their brand, contact center leaders should consider several factors when choosing the right contact center technology. To avoid the financial risks in both the short and long term, the technology contact center leaders choose must be highly secure and compliant with relevant regulations. Buyers should also consider the scalability of the technology, as well as its integration capabilities with existing systems. Additionally, buyers should look for features or compliance-related certifications such as SOC-2 compliance, robust compliant outbound campaign management built right into the technology, data encryption, multi-factor authentication, and real-time monitoring to ensure the highest level of security and compliance.

Let’s look at a few things to consider when selecting highly secure and compliant contact center technology.

Top of Mind Compliance

SOC-2 Compliance

A widely known form of compliance in not only the contact center space, but most software-as-a-service (SaaS) industries, is SOC 2. The SOC 2 – which stands for System and Organizational Controls - is a cybersecurity audit which is meant to establish trust in the service provider in that they take security and data privacy seriously. This audit is conducted by the American Institute of Certified Public Accountants (AICPA) to provide a third-party attestation that the solution provider has implemented a series of policies and procedures, and has systematically protected private information across multiple categories.

As a contact center leader, implementing an SOC 2 compliant contact center provider shows your customers that you only partner with organizations who truly care about putting security and data privacy into the core operations of their business.

STIR/SHAKEN Compliance

The rise of illegal robocalls has created a sense of distrust in consumers. STIR/SHAKEN compliance is meant to build trust in incoming phone calls and the validity of where they’re originating from. By definition, STIR/SHAKEN – which stands for Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs - is a framework of interconnected standards. This means that calls traveling through interconnected phone networks can have their caller ID “signed” as legitimate by originating carriers and validated by other carriers before reaching consumers.
For any contact center leader evaluating contact center technology, you should ask the provider if they are STIR/SHAKEN-compliant. Even if your organization is doing minimal outbound engagement, like returning a missed call from a customer, this compliance is essential to building trust between consumers and the brands they invest in.

ISO 27001 Certification
As you evaluate multiple contact center technology providers, you'll want to make sure whoever you partner with has high standards and can verify them through third-party certifications like ISO. ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 169 national standards bodies. An organization that has a recent ISO certification means they prioritize the highest quality systems and processes, helping to ensure the safety, efficiency, and consistency of their product and/or services. In other words, contact center leaders should see technology leaders who possess an ISO certification as meeting some of the strictest quality management requirements, which, in turn, means a consistent level of high-quality products and services.

Robust & Compliant Outbound Campaign Management
Gartner predicts that proactive customer engagement interactions will outnumber reactive customer engagement interactions by 2025. However, as outlined earlier, there are many regulations and laws to keep up with. This makes it challenging to ensure contact center organizations are staying within the bounds of compliant, proactive outreach. Contact center leaders evaluating this kind of technology should look for platforms with "built-in" compliance-ready tools. Look for technology that makes proactive, compliant outreach simple with functionality like compliant outbound dialing with DNC list management and dynamic list scrubbing, plus opt-out mechanisms and consent tracking that automatically updates global tables. Ensure contact center technology providers also have functionality like customizable “right time to contact” features that enable users to change default values. For example, look for technology that enables you to update a customer’s time zone based on their current postal code rather than the area code of their mobile number, which might be inaccurate. Implementing a robust, compliant outbound platform will not only reduce your risk and potential costly fines, but also enable your organization to deliver better, more positive customer connections with the ability to reach out to them at the right time and on the right channel.

Security By Design
Multi-Factor Authentication
Contact center leaders or buyers should be evaluating providers who can ensure the highest level of security using easy-to-use tools employees can adopt quickly. Contact center technology buyers should look for enhanced security functionality that requires their employees to identify themselves by more than a username and password. Although usernames and passwords are important, an added second factor of authentication can protect customers from possible data and security risks. This added layer of authentication can be given to employees via multi-factor authentication (MFA). By requiring employees to authenticate using a push notification via a mobile app or a phone call to their mobile device or softphone, for example, MFA adds an additional layer of protection against...
Unauthorized access. This significantly reduces the risk of credential-based attacks, even if passwords are compromised.

**Data Encryption**

Protecting important and private customer data should be top of mind for any contact center leader exploring technology providers. Encryption acts as a safeguard for sensitive customer data, both at rest and in transit. Contact center leaders should be on the lookout for technology providers with strong encryption protocols to protect customer information from unauthorized access. Be sure to ask the contact center partner you're evaluating if data encryption is applied to databases, file storage systems, email communications and any other channels where data is transmitted or stored. Selecting a contact center provider with the highest level of data encryption will go far into safeguarding your customers' data and therefore reducing your risk exposure.

**Security & Compliant-Driven Culture**

It's important to find a technology partner that has the right functionality to ensure a highly compliant and secure contact center environment. But what can set one provider apart is having a security-first culture from the inside out. Contact center leaders can go one step further in selecting the right technology provider by looking into a vendor's internal organizational structure, seeing how the company prioritizes experienced security professionals who are meeting with executive staff to continue investments in the latest security enhancements at scale. Contact center leaders evaluating this type of technology should also consider a provider's security team itself and the number of decades of experience the IT and security team has as well as how many members of the team have top-notch security certifications like CISSP (Certified Information Systems Security Professional).

**Real-Time Protection**

Even with a culture of heightened security awareness, sophisticated cybersecurity attackers may still pose a risk. Contact center leaders should do their due diligence in seeking out a partner who can provide real-time protection from nefarious actors. Highly secure contact center providers can automatically block IP addresses who are continuously attempting to execute suspicious activity, for example. This means this kind of real-time protection no longer relies on human intervention but can be done immediately, providing 24-hour, around-the-clock protection. Or, from a firewall perspective, partner with a leading security-first contact center provider to enforce geofencing, which blocks IP addresses from countries that malicious activities are known to originate from, protecting your network from potential threats.

**Alvaria Is Here to Help**

In today's world, data privacy and security are critical concerns for organizations of all sizes. Contact centers are a hub for sensitive information, and as such, highly secure and compliant contact center technology is essential for contact center technology buyers and the organizations they support. Failure to prioritize contact center security and compliance can lead to significant financial and reputational damage. We understand that organizations are faced with the challenge of finding the right highly secure and compliant technologies to reduce these risks. Alvaria stands ready to assist our customers with the latest and greatest security and compliance features and functionality as well as a security-first culture with the right expertise to protect your sensitive customer information and meet regulatory requirements.