PCI Compliant Call Centers are industry leaders in 2023

Call center operations have gone through a lot of changes over the past few years, and PCI compliance is one of them.

PCI or Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment of performing and processing transactions.

PCI Compliance Standards protect sensitive customer data from being compromised by cyber attackers. Moreover, a **PCI compliant call center** is more likely to attract a larger consumer base as opposed to call centers that are not compliant.

This article will elaborate on why it's so important for call centers to be PCI compliant, the risks associated with not being PCI compliant, the steps in becoming PCI compliant, and how a **PCI compliant call center** can benefit from PCI DSS compliance.

The Importance of PCI Compliance in Call Centers

PCI compliance is essential for the call center industry for the following reasons:

- PCI compliance ensures that the consumer's personal data such as the credit card number and other sensitive information is kept safe. A **PCI compliant call center** agent will never ask a customer directly for their credit card information.
- A **PCI compliant call center** can also avoid heavy fines and penalties that are enforced by the PCI DSS security council on non-compliant contact centers.
- Moreover, a **PCI compliant call center** builds trust within customers, assuring them that their transactions are secure and protected by strict security protocols.

In addition to these benefits, A call center can also benefit from PCI compliance in the following ways:

- It's easier to detect fraudulent activity in a **PCI compliant call center** when there's a standard format for reporting breaches, or if there are rules governing how many times an employee can access sensitive data without going through additional safeguards such as two-factor authentication.

- In every **PCI compliant call center**, fraudulent activity associated with credit card transactions is automatically detected and filtered out.This makes it harder for cyber-criminals, who might try using different methods like phishing emails or malware attacks against businesses with less strict security protocols and policies.
- A **PCI compliant call center** is also less likely to be a victim of a mass data breach. Data breaches can be very costly for businesses, and may damage their reputation for a long period of time.

Finally, PCI compliance helps you prevent fraud by showing customers that you're committed to security. It shows them that their data is safe with you and makes them more likely to choose a PCI compliant call center over a contact center that isn't compliant.

Is PCI Compliance necessary for all merchants?

For the purpose of PCI compliance, all merchants that accept credit cards are considered "card-not-present" (CNP) merchants. To be a CNP merchant, you must have a merchant account and accept payments from customers who don't have their card physically present with them while they are making purchases. Additionally, it is also necessary for a service provider to be PCI compliant in order to ensure legal and secure transactions from one channel to another.

A service provider is any organization that processes data for use in the development or operation of an application or service provided by another entity. This includes services such as hosting and storage of data, but does not include network infrastructure providers like ISPs, wireless carriers and cable companies who just pass traffic through their networks without doing anything else with it ,although they may also perform other related functions.

In addition to these types of providers being subject to PCI compliance standards, they should also be aware that they themselves could become targets if they fail to comply with these regulations.

Having a service provider that has been breached can be very damaging to your business. If your company is the victim of a data breach caused by a third party, they could be held liable for damages incurred by any individuals whose information was exposed in the incident.

Risks associated with not being PCI compliant

DoS Attacks

A DoS attack is a denial of service attack, which occurs when an attacker uses resources to prevent legitimate users from accessing their intended websites and services.This can be done by overloading the system with requests, or by flooding it with traffic that it cannot handle.

The latter type of attack is common in call centers where there are many different agents being asked to perform different tasks at once (e.g., one agent may be handling customer questions while another is making outgoing calls).

In a **PCI compliant call center**, call center systems and databases are secure from DoS attacks, as they are protected by PCI DSS security protocols and standards, implementing an additional layer of security against all forms of DoS attacks.

Call Center Phone System Vulnerabilities

A call center phone system vulnerability is a type of risk that can be exploited by an attacker to gain access to your call center system. Call centers that are running outdated versions of Windows, Macintosh and other operating systems are the most vulnerable to these security risks.

If you suspect that your company has a call center phone system vulnerability and haven't taken any steps yet to fix it, there are several things that you can do:

- Update all employees' computers with Microsoft patches as soon as possible; this includes both desktops as well as mobile devices (iPhones and Android phones).
- Implement anti-virus software on all computers in use at the company so they don't become infected by malware while they're using them while they're connected via Wi-Fi networks at the office or home.
- This may also include installing malware protection software onto laptops used outside of normal business hours where no internet connection is available—like if someone travels somewhere without access online such as traveling abroad during vacation time off from work.

Credit Card and Payment Processing Fraud

PCI compliance is important to protect your customers and your company from fraud and other scams. It helps ensure that you are not vulnerable to data breaches, which can have a negative

impact on your brand and reputation. In addition, it protects your employees from identity theft or phishing attempts by making sure they know how to identify fraudulent emails or phone calls.

As an example, let's look at one of the most common ways criminals try to trick call center agents: spoofing caller ID information so that they appear as though they are calling from within your organization (this is called Caller ID Spoofing). If a customer receives a call from what looks like their bank asking for sensitive information like their Social Security Number or PIN code over the phone, there is no reason not to give it--and this type of attack has been happening more frequently in recent years.

This makes PCI compliance even more important because it will help prevent these types of attacks by ensuring all employees know what legitimate companies should look like when they interact with them digitally--and how those interactions should go down.

Four levels of PCI Compliance

The PCI Security Standards Council defines **four** levels of compliance depending on the credit card transactions performed by your business. These levels are:

Level 1: This level includes merchants and organizations that make and process transactions equal to 6 million card transactions in a year.

Level 2: Level 2 of PCI compliances includes merchants and organizations that process about 1 to 6 million card transactions in a year.

Level 3: This level of PCI compliance includes organizations and merchants that process around 20,000 to 1 million transactions in one year.

Level 4: Level 4 of PCI compliance is for organizations and merchants that process less than 20,000 transactions in a year.

The latest call center PCI compliant requirements include changes to address phishing attacks, network security controls and cloud computing. The new requirements are aimed at preventing fraudulent activity that could occur as a result of weakly secured networks, applications and data stored in the cloud.

PCI DSS Requirements for PCI Compliance

Call centers have PCI DSS requirements for call recording, file transfers, and encryption according to level of transactions. According to the Payment Card Industry (PCI) Security Standards Council, "the most critical data elements are stored in a database that supports credit

card processing transactions." That's why it's important for companies that process payments through their call center to ensure their systems are secure against potential data breaches.

Call centers must adhere to PCI DSS standards related to protecting customer information by using encryption when transmitting sensitive data over public networks such as the Internet; storing all credit card numbers in an encrypted format; maintaining regular inventories of portable digital media containing cardholder information; restricting access only employees who need it; training employees on how not to lose or mishandle sensitive information (e.g., passwords).

In the wake of high-profile data breaches, including those at Target and Home Depot, companies that process payments through their call center must ensure their systems are secure against potential data breaches.

Call centers must adhere to PCI DSS standards related to protecting customer information by using encryption when transmitting sensitive data over public networks such as the Internet; storing all credit card numbers in an encrypted format; maintaining regular inventories of portable digital media containing cardholder information; restricting access only employees who need it; training employees on how not to lose or mishandle sensitive information (e.g., passwords).

PCI Compliance is the need of the hour in 2023

Call center operations are critical to the success of a business. While call centers provide an important service to various industries requiring call center assistance, they are also presented with a unique set of challenges in terms of security and compliance. Credit card and payment fraud can be costly for businesses, so it's important for you to always ensure that you are trusting **PCI compliant call centers** only.

Call center security is essential for maintaining compliance with regulations such as PCI DSS (Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability & Accountability Act). Despite their distinct set of requirements, these standards require specific measures be taken by organizations which handle sensitive information like credit card numbers or medical records. They also help ensure that companies have adequate safeguards against cyber attacks so they don't lose sensitive data that could result in financial loss or identity theft if compromised by hackers.

Credit card and payment fraud can lead to costly consequences. For example, if a call center employee is caught using a customer's credit card number for personal gain, it could cost your business. Not only do you stand to lose customers who may be angry about their information being used without permission, but you could also face fines from regulators and lawsuits from

individuals who have been victimized by identity theft or other crimes that resulted from the breach of their sensitive data.

Touchstone Communications - A PCI Compliant Call Center

Call centers are a key part of any organization or, and PCI compliance is essential for their security. Call centers have many responsibilities that require that they be PCI compliant, such as handling sensitive payment and credit card information from customers. Many companies do not realize the importance of this step in protecting their business from fraud or other scams until it's too late.

Touchstone Communications is a **PCI compliant call center**, where every transaction is a secure transaction. Our wide range of **omni channel BPO services** include payment and transaction processing, **customer services outsourcing**, **omni channel inbound services,** and **outbound lead generation services.**

Our **PCI compliant call center** is also ISO 9001 certified, where we insure industry best practices to prevent credit card fraud and theft.

We enhance customer experiences by providing secure payment solutions for our clients. We offer customized systems and services with strong security and scalability requirements that meet or exceed PCI standards and are PCI compliant.

You can learn more about how our **PCI compliant call center** at Touchstone Communications works by connecting with us today.

Frequently Asked Questions

Q. **What is PCI Compliance?**

Ans. PCI compliance is a set of security standards for protecting credit card data. It's required by the Payment Card Industry Security Standards Council (PCI SSC), which oversees the implementation and enforcement of these standards.

Any organization that processes, stores, or transmits credit card data must be PCI compliant in order to prevent security breaches like those at Target and Home Depot--and even smaller businesses need to take steps toward achieving compliance if they handle sensitive customer information such as credit card numbers, name of the credit card holder and expiry date.

Q. How much do I have to pay to be PCI Compliant?

Ans. As a business owner, you often must pay a fee to your card processing provider (like Visa, MasterCard or Discover) to achieve PCI compliance. The cost is generally around $70-120 annually, though it can be higher or lower depending on where you are located. You'll see this charge reflected on your processing statement.

By entrusting your business operations to a **PCI compliant call center**, your business will not have to pay a fee to ensure secure transactions, as the annual fee for compliance would be paid by the **PCI compliant call center**.

Q. Why is PCI compliance important?

Ans: PCI compliance is a requirement for all organizations that process, store or transmit credit card data. If you have an online store and accept payments through your website, it's important to be PCI compliant.

The same goes for any business that accepts payment cards in person (like a retail store). Additionally, when companies outsource their operations to a contact center, they would want to ensure that they are outsourcing to a **PCI compliant call center**.

Q. **Is there any PCI compliant call center software?**

Ans. No. There isn't any specific **PCI compliant call center** software, as the PCI DSS is a set of security standards that must be met by call centers to perform legal and secure credit card transactions. However, existing call center technologies can be integrated within **PCI compliant call center**s to deliver a secure customer experience.

Q. How does PCI Compliance work?

Ans. PCI Compliance is a way to ensure card holder's data integrity during the online use of credit cards. PCI DSS is a reiterative process that involves assessing and analyzing cardholders' data for any data exposure risk and fixing the loopholes vulnerable to attack.

This process helps keep the data and sensitive information of the client secure against attacks during online transactions. It is important to make sure that the companies you do business with are PCI Compliant.

Touchstone Communications is a **PCI compliant call center** which means every transaction made and all the data handled is safe and secure. Get the highest level of data security for your valued clients with our **PCI compliant call center**

Q. **What happens if a call center is not PCI compliant?**

Ans. There are many consequences of noncompliance with PCI standards. The most obvious is that your organization may lose business, customer trust and revenue. You could also suffer a loss of reputation as well as customers, business partners, employees and investors. Suppliers and vendors may also choose not to work with you because they don't feel safe dealing with companies whose security measures aren't up to snuff.

On the other hand, a **PCI compliant call center** is more secure, reliable and meets all compliance standards to conduct secure credit card transactions.