Create Contact Center Experiences Your Customers Can Trust

interactions

Put TRUST Back into Customer Relationships with PCI-Compliant Credit Card Transactions

You made it through the pandemic. Now you need to stay compliant in this new hybrid environment. The work-from-anywhere (WFA) agent is the post-COVID reality for contact centers around the world.

The stakes are higher than ever. Data breaches have increased in number and severity, directly impacting revenue due to penalties and fines while eroding brand reputation, customer loyalty, and trust.

interactions.com/products/trustera/

trustera@interactions.com

What is a data breach costing you?

44% of data breaches include Payment Card Information (PCI) or Personally Identifiable Information (PII).

$500 million is the overall cost of one data breach settlement—without including the major hit to brand equity.

$5 million is the cost of a breach involving a remote worker, $1 million more than where remote working is not a factor.

Similarly, according to the 2022 IBM Security Cost of Data Breach Report:

83%

Organizations studied that have had more than one data breach.

60%

Organizations' breaches that led to increased prices passed on to customers.

19%

Frequency of breaches caused by stolen or compromised credentials, the most common cause of a data breach.

More than money

The PCI Security Standards Council, regulatory agencies, and credit card brands can administer hefty fines and penalties.

Forensic investigations can be expensive.

Future security costs can mount up and include compulsory credit monitoring, card replacement, and identity repair.

There are also hidden costs, like legal fees, PR campaigns, and insurance premium hikes.

A single data breach can cost a brand its reputation. Customers lose trust, taking their business elsewhere.

Set up your agents for success (and security) wherever they are

Ensuring secure transactions for customers is a key focus as the use of credit and debit cards continue to remain a popular form of payment in this digital age. The introduction of credit card security for in-person transactions (e.g., EMV embedded chips) and online card-not-present transactions (e.g., 3-D Secure authentication) has been essential in making customers feel at ease when making purchases.

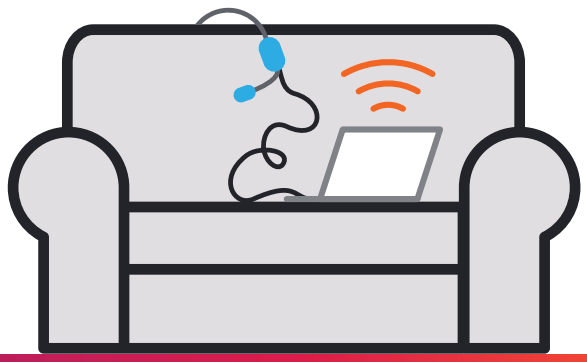
However, phone transactions still remain one of the top three ways that people buy goods and services and most contact centers require consumers to read their credit card numbers aloud to a live agent. With the agent workplace also continuing to evolve, agents may be onsite, but could be staffed as part of a hybrid or work-from-anywhere model. This can leave the security of cardholder data vulnerable and present a significant PCI compliance risk to your employees and your business.

HOW WFA FACTORS INTO PCI COMPLIANCE

Due to cost reduction, high attrition rates, and labor shortages, contact centers continue to rely on a growing work-from-home (WFH) agent workforce. Gartner Research projects that the customer experience WFH workforce will increase to 35% by 2023, posing additional risks for sensitive customer data breaches.

While most contact centers have implemented safeguards to prevent on-premise agents from accessing sensitive information–clean desk policies, video camera surveillance, strong access control measures, regular network monitoring and testing–none of these guarantee full compliance and protection. And, as the workplace continues to extend beyond the controlled contact center environment to a WFH or hybrid model, most of these controls cannot be enforced offsite. Additional PCI compliance controls are required to protect PCI collected by WFH agents, and agents must be trained on proper behavior.

However, a 2020 IBM Work From Home Study during COVID reported that agents had not received proper training on handling PII while working from home, and 42% of United States-based respondents reported working with PII in their job. Companies are now playing catch-up to bring WFH agents into compliance.



interactions.com/products/trustera/

trustera@interactions.com

Confronting Contact Center Compliance Issues

With the cost of fraud increasing to $3.75 for every $1 stolen in 2022, CISOs and contact center executives are actively confronting this problem. Contact centers are beginning to turn to technologies that enable agents to collect cardholder data without needing to copy down the data. While several solutions exist to securely collect cardholder data, PCI compliance is guaranteed only when the agent manually turns it on. The remainder of the call remains vulnerable, and there are no monitoring controls to ensure that agents do not attempt to collect the data using other means. Since the purpose of PCI compliance is to avoid the mishandling of cardholder data, current technology solutions do not eliminate the risk of fraud caused by bad actors, and contact centers remain exposed.

Using Dual Tone Multi-Frequency (DTMF) suppression.
The agent directs callers to use their touchtone phones to key in their credit card numbers. The audio is masked, so the agent only hears pulse sounds. However, agents must initiate the process by manually setting it up on their terminal to receive the numbers. The caller must key in the numbers, which statistically has a higher likelihood of mistakes than speaking.

Using a different channel to redirect customers to a secure form.
The agent may send the caller a link to their smartphone to a payment website. This approach requires increased customer effort and significantly lengthens the average handle time (AHT).

Transfer the call to a secure IVR (or similar) for PCI capture
This task requires well-trained agents and no bad actors in the agent pool.

Transferring the call to on-premise.
Some companies prevent work-from-home agents from accessing payment screens, which means they must transfer payment-related calls to on-premise agents.

Trust in a Better Way: The Trustera Way

There is an easy-to-use solution that does not require customers to enter card details into a phone keypad or where agents see or hear sensitive information—an approach where payment information is PCI compliant.

Interactions Trustera is a real-time AI-powered redaction system that immediately recognizes when a customer is about to share sensitive information and redacts it. The sensitive data automatically populates into the destination systems. For the customer, the process is transparent. Agents never hear sensitive information, ensuring a secure transaction.

Trustera enables these conversations to comply with PCI-DSS and PA-DSS requirements, regardless of where an agent works. The experience is seamless and uninterrupted.

TRUSTERA BENEFITS

Redacts PCI spoken by the customer so that the agent does not hear it.

Auto-collects the data in a protected database.

Confirms the PCI data has been collected successfully so the agent can continue the call.

English and Spanish (more languages coming).

Leverages and seamlessly integrates with existing order processing systems.

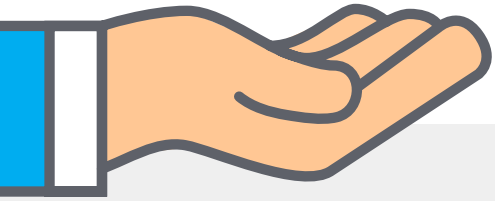
Get in touch with Interactions to learn more about how Trustera can benefit your contact center.

Trustera: Protecting Your Contact Center and Customers

Trustera is already proving itself in the market as the first-of-its-kind redaction platform. Trustera monitors calls by default and protects PCI immediately as it's spoken. Agents don't have to remember to turn it on and they can't circumvent it without explicit authorization.

To date Trustera:

- Has protected millions of credit cards annually
- Has supported 15,000 agents weekly
- Offers a 97% solution success rate, with >95% PCI redacted
- Reduces AHT by up to 60 seconds compared to alternative solutions



In addition to providing secure and compliant transactions, value-added services enabled by Trustera include:

- **Redacted audio recordings and speech transcription:** Enables calls to be securely shared and prevents unauthorized access to PCI.
- **Secure third-party integration support:** Real-time agent assist, sentiment, analysis, and post-call analytics.
- **Call protection in English and Spanish.**

About Interactions

Interactions provides Intelligent Virtual Assistants that seamlessly assimilate Conversational AI and human understanding to enable businesses to engage with their customers in highly productive and satisfying conversations. With flexible products and solutions designed to meet the growing demand for unified, omnichannel customer care, Interactions is delivering unprecedented improvements in the customer experience and significant cost savings for some of the largest brands in the world. Founded in 2004, Interactions is headquartered in Franklin, Massachusetts with additional offices worldwide.

For more information about Interactions, contact us:

trustera@interactions.com
interactions.com/products/trustera/

interactions

interactions.com