West takes you beyond PCI compliance to eliminate the risk of fraud in your call center.

CallGuard removes sensitive numeric data from all areas of your contact center environment including call recordings, agents, networks, databases and processes. This includes credit card information, social security numbers, date of birth (DOB), private health care information or any other sensitive numeric data.

CallGuard’s hosted service is ideal for organizations that have a call center or outsource call center services, both locally and around the world. It intercepts sensitive data at a network level, ensuring no sensitive data reaches any part of the contact center or your agents.

Let West help you reduce the time and ongoing costs associated with complying with more complex and evolving regulatory mandates.

**$5.85 Million**

is the average cost of a data breach in the U.S.*

*2014 Cost of Data Breach Study, Ponemon Institute, May 2014

---

**Why Choose CallGuard Hosted?**

1. Agent assistance and call recordings may continue throughout the transaction process.
2. Sensitive data is stopped before entering the network, protecting your entire call center from fraud.
3. Eliminates the unknown costs associated with future regulatory mandates.
4. No on-site equipment required.

Improve your current and future compliance and risk profile, no matter how mature it is today.
Stop sensitive data from reaching your call center environment

How it works

All incoming calls to your contact center come through the platform in the network. The platform sends an identification number to your contact center agent with every new call. The agent types this number into the CallGuard web payment interface on their desktop to begin the transaction process.

CallGuard allows the caller to remain on the phone with the agent through the transaction in the event the caller has any difficulty or wants to complete any final tasks.

When payments or sensitive data is required the agent asks the caller to enter the numeric data using their telephone keypad, which will generate Dual Tone Multi Frequency (DTMF) tones.

CallGuard recognizes these tones as sensitive information and replaces them with flat tones to allow the call recording to continue. The agent’s desktop displays payment progress indicators. The flat tones and indicators mean there are no implications to PCI.

The hosted platform handles both card authorization with the Payment Service Provider and settlement, and the agent soon advises the caller of their authorization code.

CallGuard ensures that while sensitive data remains isolated from the contact center environment, the agent and caller can continue dialogue at all times, providing a seamless customer experience.

---

Stage 1
The caller rings the contact center to inquire about a product or service. Call recording can continue throughout the entire conversation, including taking a payment.

Stage 2
The caller enters their card details using their telephone keypad. DTMF tones are intercepted by CallGuard and changed to monotones. The web screen masks the digits from the agent as the customer presses the buttons.

Stage 3
CallGuard checks the details directly with the Payment Service Provider. The agent is notified of payment approval or rejection. At any stage of the process, the agent can cancel and start again while the customer is on the phone.

---

KEY BENEFITS

- CallGuard Intercepts phone DTMF tones, capturing card data in our hosted environment.
- Improve customer experience and increase trust; your customers no longer need to worry about providing their sensitive information over the phone.
- Agents cannot see, hear or access card details at any time, but can speak to the caller during and after payment.
- Tokenization available to allow repeat payments.
- Agents can take payment regardless of locality (home-based, off-shore, etc.)
- Fully integrated with existing CRM and/or Payment Service Provider.