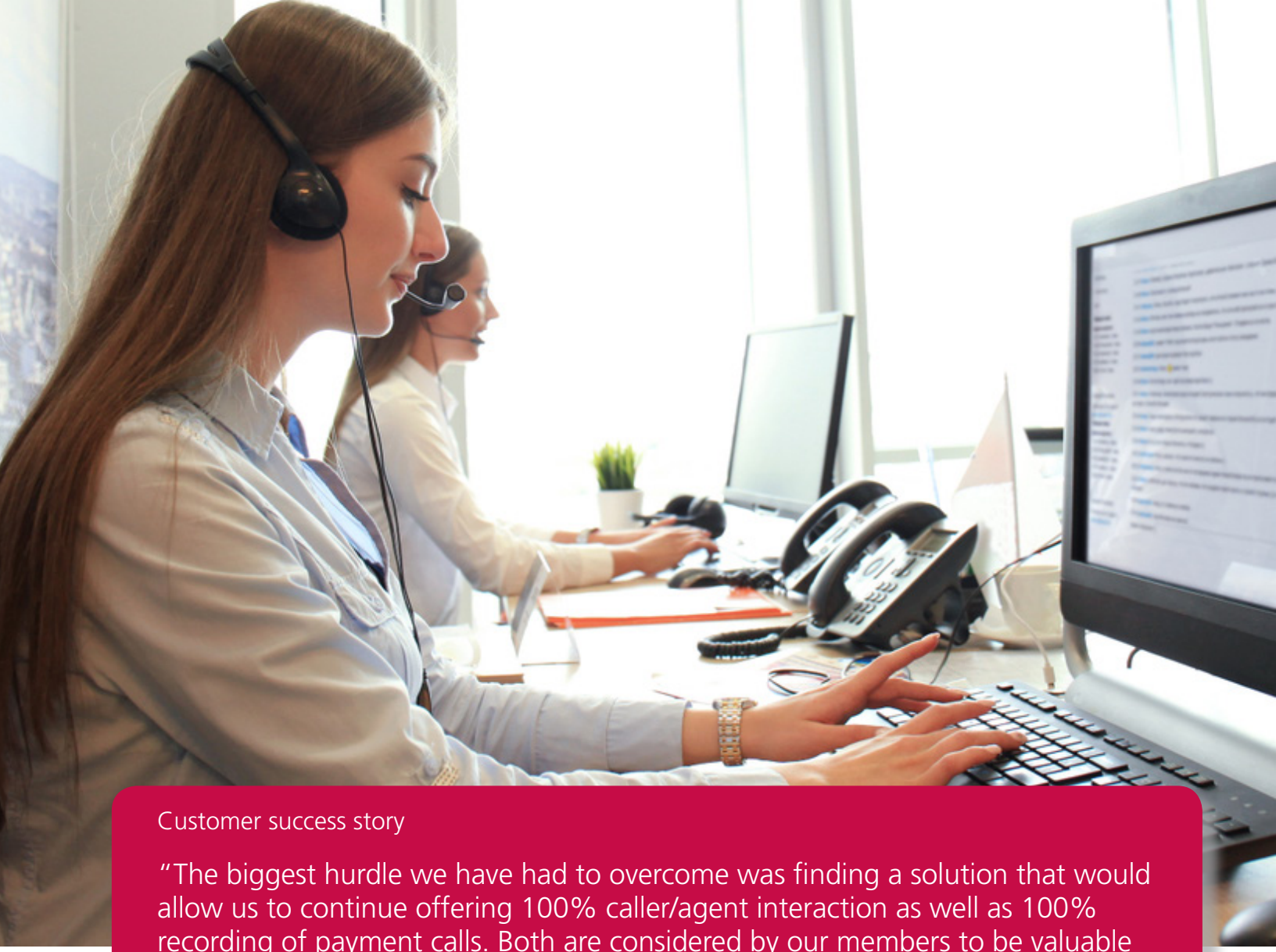

Customer success story

"The biggest hurdle we have had to overcome was finding a solution that would allow us to continue offering 100% caller/agent interaction as well as 100% recording of payment calls. Both are considered by our members to be valuable cornerstones of CRC's services and our answer was found in CallGuard."

Paul Thompson, Vice President of Administration/CFO, Cooperative Response Center, Inc.

CRC
Cooperative Response Center, Inc.

Securing customer payments by preventing sensitive data being stored or accessed.

PROFILE: Industry: Business Services **Employees:** 300 **Turnover:** US$ 12.5 million

BUSINESS

A nationwide, cooperatively owned and operated 24x7 contact center, central station and software provider.

CHALLENGE

To achieve and maintain PCI DSS compliance across the enterprise to secure the thousands of incoming payment calls.

SOLUTION

CallGuard for agent-assisted payments and PCI DSS compliance.

BENEFIT

1. Speedy implementation
2. No sensitive data is available for criminals to steal or recorded
3. Agent and customer remain in contact throughout the interaction.

The background

Founded in 1992, CRC has steadily increased in the size and scope of its operation with offices in Austin, MN, Dunlap, TN, and Abilene, TX. We provide services to electric utilities, including round-the-clock dispatch and customer care, and monitoring of security and medical alarms. CRC currently serves over 450 members and associate members in 45 states, representing over 8 million consumers.

The value

CRC rolled out CallGuard in a very short time of just three months. The solution now enables contact center agents to take sensitive information from customers without seeing or hearing any data being verbally relayed to them.

This means that CRC agents are not burdened with data that they do not need to see and CRC has greater control over the information that their customer facing staff have access to. This assures their clients' data and their consumers' data is protected.

Initial concerns that customers would find it strange to enter their numbers using their keypad rather than speaking them were soon eradicated. End consumers actually appreciated the new and extra security measures taken to secure their personal data and had absolutely no issues with relaying their data in this way.

The challenge

With thousands of calls coming in from customers relaying credit card details, CRC needed a method that would comply with PCI Data Security Standards across the enterprise, but maintain their high level of customer service. CRC wanted to change the process of capturing credit card numbers and security codes from being spoken by the caller and then entered by the agent, to being keyed into the phone by the caller and captured by the agent's PC.

Whatever solution was chosen, it needed to be implemented quickly, without disruption to the existing IT infrastructure and run smoothly. It also needed to be flexible enough to meet client's customer service standards.

The solution

CallGuard On-Site was presented to CRC who needed to know how it was going to work operationally from a contact center perspective. They also needed to know how well it would integrate with other IT and Telecoms within the business.

After the proof of concept was approved, CRC implemented CallGuard across the entire enterprise, across multiple desktops and programs. This all took place in just a couple of months.

A Decoder was installed on each desktop and phone which encrypts the card details before they enter the agent's screen. The agent only hears the sound of the numbers being keyed in (DTMF tones). A Filter was also installed next to the CRC call recorder to remove the DTMF tones made through the keypad and replace them with flat tones.

Finally, DataShield was uploaded onto the agents' desktops to mask the card data from appearing on the screens as the Decoder interprets the pressed keys into numeric data entry. These fields cannot be accessed by agents and ensures that the information cannot be communicated, stored or written down.

At the end of the call the caller and agent have been engaged 100%, the entire call is recorded, and there is no Cardholder Data or Sensitive Authentication Data stored in the call recording.