The State of Data Security in Contact Centres

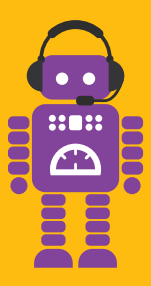
semafone
securing data · protecting reputations

Contact centre agents and customer service representatives rely on broken, risky processes to collect payment card data and other personally identifiable information (PII) over the phone:

72% of agents still require customers to **read card numbers out loud**

=

Increased Risk of Exposure



11% use “other” methods, like interactive voice response (IVR) systems

=

Poor Customer Experience

10% capture data through an online chat window

=

Agents and Computer Applications Still “Touch” the Data

30% of agents have access to customers’ payment information or social security numbers on file **even when they’re not on the phone with the customer**

More than 40% of agents *do not report* breach attempts

When this information is accessible to agents, organisations are at risk of a data breach:

Agents are unlawfully sharing and being asked to share customer data

9% of agents personally know someone who has unlawfully accessed or shared customer information

7% have been approached by someone inside their organisation to share sensitive data

4% of agents have been approached by someone outside their organisation to share sensitive data

Europe VS. North America

0 have been approached by outsiders to share information

16% have access to customer information when they aren't on the phone with them

2% have been approached by outsiders to share information

With approximately 2.2m agents in the U.S. these findings indicate it is possible that close to 150k active agents in the U.S. have been asked to share sensitive customer data by others within their company; and more than 85,000 agents may have been approached by an outsider to share information.

31% have access to customer information when they aren't on the phone with them

Fortunately, They Can’t Hack the Data You Don’t Hold:

It’s easy to keep sensitive information out of the contact centre altogether. Cardprotect from Semafone allows your customers to enter their payment card numbers directly into their telephone keypad instead of saying them out loud over the phone. They can stay in conversation with the agent because DTMF masking "disguises" the card numbers so they can't be identified by their sound. That means sensitive payment card data isn't captured on call recordings and other contact centre systems and agents can't hear or see card numbers either.

Based on Semafone's State of Data Security in Contact Centres Agent Survey and Report

Contact us now on 0845 543 0822 for more information.

www.semafone.com info@semafone.com @semafone Semafone