THE STATE OF DATA SECURITY IN CONTACT CENTRES

Analysis by

semafone®

securing data · protecting reputations

Contents

INTRODUCTION

With data breaches and cyber attacks occurring almost daily, organisations are looking to strengthen their data security practices to better protect customer data and avoid the reputational damage of an embarrassing public data breach.

Yet, one area of vulnerability is often overlooked when it comes to protecting data: the contact centre. Since the widespread adoption of the EMV chip card, fraudsters have been shifting their focus to card not present (CNP) channels, such as contact centres – often deemed "low-hanging fruit." And, with personally identifiable information (PII) – including credit and debit card numbers, sensitive authentication data (SAD), social security numbers (SSNs) and more – regularly flowing through their IT environments, contact centres are especially attractive targets. To gain first-hand insight into the state of data security in the contact centre, Semafone conducted an anonymous global survey of contact centre agents across multiple industries, gathering more than 500 responses.

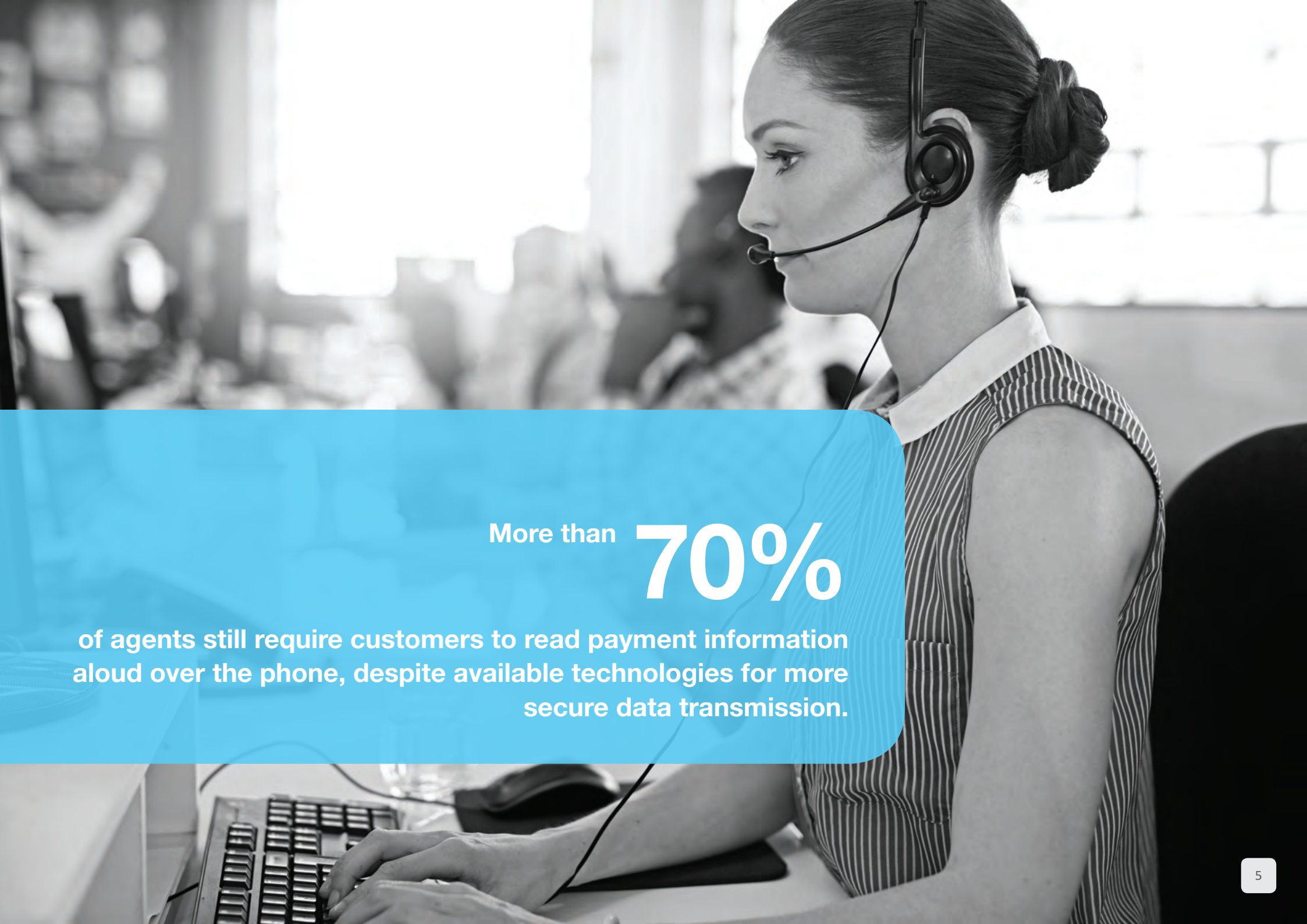
EXECUTIVE SUMMARY

This survey shows that a concerning number of contact centres continue to rely on outdated, risky practices for customer interaction, data collection and fraud prevention. For example, more than 70% of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission. At the same time, a disconcerting number of agents have been approached directly by company insiders and/or outsiders to share customer information.

Survey findings emphasise the urgency for contact centres to secure all sensitive data and reduce the risk of brand-damaging data breaches. Current security measures, such as the use of clean rooms (no writing utensils, paper, phones or bags) and checkpoints for agents are not enough. While there is reason to believe that not all agents have fraudulent intentions, it is important to understand that it takes just one malicious person – coupled with poor data security – to send an organisation into a downward spiral.

Recommended solutions for mitigating contact centre security risks include: more robust incident management policies; proper access controls for computer systems; tokenisation technologies that replace data with a meaningless equivalent; and dual-tone multi-frequency (DTMF) masking technologies that shield data from agents as customers enter it into their telephone keypads.

However, the best way to protect customer information, deter fraud and safeguard a company's reputation is to remove sensitive data completely from the contact centre environment.



More than **70%**

of agents still require customers to read payment information aloud over the phone, despite available technologies for more secure data transmission.

Key statistical findings from this survey include:

Contact centres still rely on outdated and risky data collection and customer interaction practices.

72%

of agents who collect credit or debit card information over the phone said they still require customers to read payment card numbers out loud, despite the readily available technologies that secure voice transactions

30%

of agents reported that they have access to customers' payment card information on file even when they're not on the phone with the customer

Agents are experiencing and witnessing breach attempts from both insiders and outsiders, yet many do nothing to mitigate the risks.

7% of agents admitted that someone *inside* their organisation had asked them to access or share customers' payment card information or other sensitive data

4%

said the same about someone *outside* their organisation

9% said they personally know someone who has unlawfully accessed or shared customers' payment card information

42%

of agents who were approached said they did not report the situation

Contact centres aren't doing enough to protect customer data.

26%

of agents said they work in a contact centre "clean room," which prohibits personal items and recording devices of any kind

38%

of agents are not allowed paper or pens at their work station

31% of agents are not allowed personal items or bags at their work station

28% of agents are required to pass through a security check before entering or leaving work

Industry and geographical trends are apparent.

0 European agents reported instances of outsiders approaching agents to share information – likely reflective of Europe's stricter governance rules

50% of agents in Central and South America have access to customer data when they aren't on the phone with the customer. These regions also had the highest number of requests to share data

35%

of agents in the Business Process Outsourcing (BPO) industry have access to customer information when they aren't on the phone with them; and **11%** said an insider had approached them to share customer information

The above findings point to increased risks due to outsourcing and offshoring, making strong data security even more important for contact centres with such business models.

semafone®
securing data · protecting reputations

To read the full report, please visit our website to download the complete file.

Read the Full Report Now

0845 543 0822
info@semafone.com
www.semafone.com
@semafone
Google+
LinkedIn
Pannell House, Park Street, Guildford, Surrey, GU1 4HN