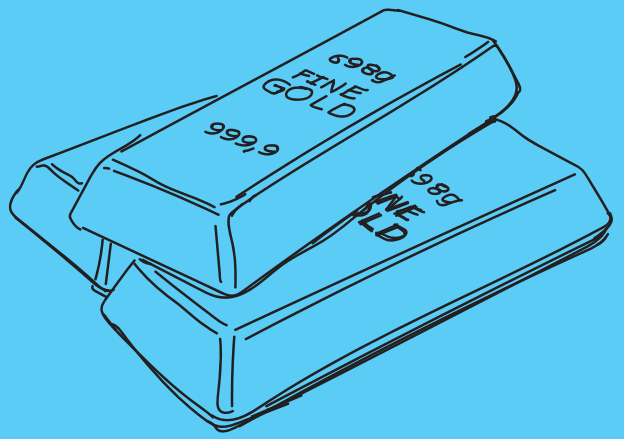
semafone®
securing data · protecting reputations

THE FLAWED FIVE

Personal information today is pure gold to fraudsters. Demographic details alone are highly valuable and sensitive information, such as credit card numbers or user IDs and passwords, are worth a great deal on the black market.

In fact, a single stolen credit card number currently sells for around £25 on the dark web. Little wonder then that contact centres are a prime target for fraudsters, who are persistently – and ingeniously – looking for new ways to get their hands on your customers' data.

You may think you have invested in sufficient technology to protect your contact centre and comply with industry regulations such as the Payment Card Industry Data Security Standard (PCI DSS), but are you confident that you have the right systems, processes and people to stay one step ahead of the fraudsters? And have you given enough thought to insider threats?



The vast majority of customer service agents are diligent, customer-focused and trustworthy.

If they are handling sensitive data such as credit or debit card details, however, they could pose a risk. Anyone working in your organisation may be subject to bribery, threats or trickery; and if you have temporary staff covering seasonal peaks and troughs in demand, employ home-workers or use contractors to maintain your building or your IT systems, that risk is even higher.

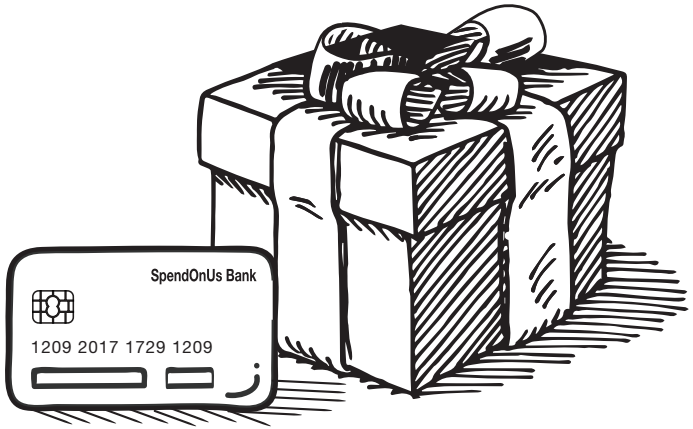
Meet five characters who could pose a security risk to your contact centre…

Opportunistic Oscar

The Tempted Temp

Oscar is one of the many students who works in your contact centre over Christmas. He's a nice guy, but he doesn't over-think things. He's surprised that people are providing him not only with card numbers, but also CVV codes and addresses over the phone. He decides to write a few of them down.

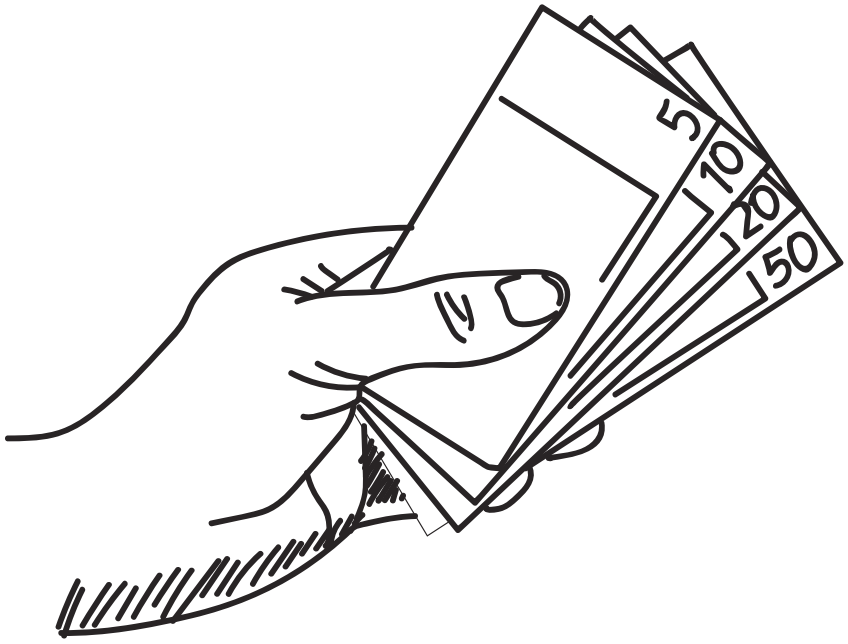
One evening, while working on the night shift, Oscar treats a group of his contact centre colleagues to a late delivery of pizzas courtesy of one of the card numbers he's taken. He knows that the credit card company will pick up the bill, so doesn't feel too guilty. Also, he isn't very worried about getting caught as he's only employed by the contact centre for a few weeks and then he's back to university. Oscar's scheme works so well that he uses a different card to buy a camera online the next day, and another to buy a new laptop the day after that.



Unfortunate Ursula

The Credulous Clicker

Meanwhile, Ursula, a diligent customer service agent, is busy responding to customer emails, resolving complaints, answering questions and facilitating account changes. She comes across an email from a customer about a damaged product. The email comes with an attachment which Ursula believes to be a photograph to back up the claim. She clicks on it. Unfortunately, entirely without her knowledge, this installs a malicious worm that spreads swiftly across your contact centre's IT network, stealing customers' data and transmitting it to fraudsters operating from the outside.



Disgruntled Daisy

The Vengeful Victim

Daisy has worked loyally in your contact centre for 10 years, but she is not happy. A clean room policy (no phones, bags or writing materials at her work station), is due to be put in place because Oscar was caught writing down card numbers. For Daisy, this made it impossible to continue in her sales and customer service position.

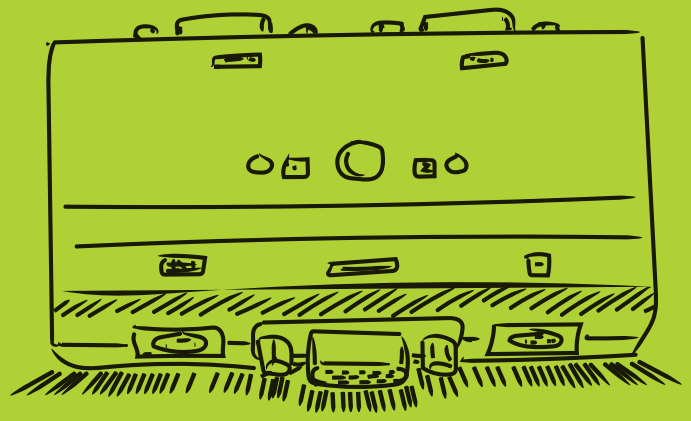
She has young children, and couldn't be cut off from her mobile phone in case her children were taken ill at school or got into trouble. She has moved to an admin role instead, without any of the sales commission she used to depend on. She feels hard done-by and is desperate to find some additional income.

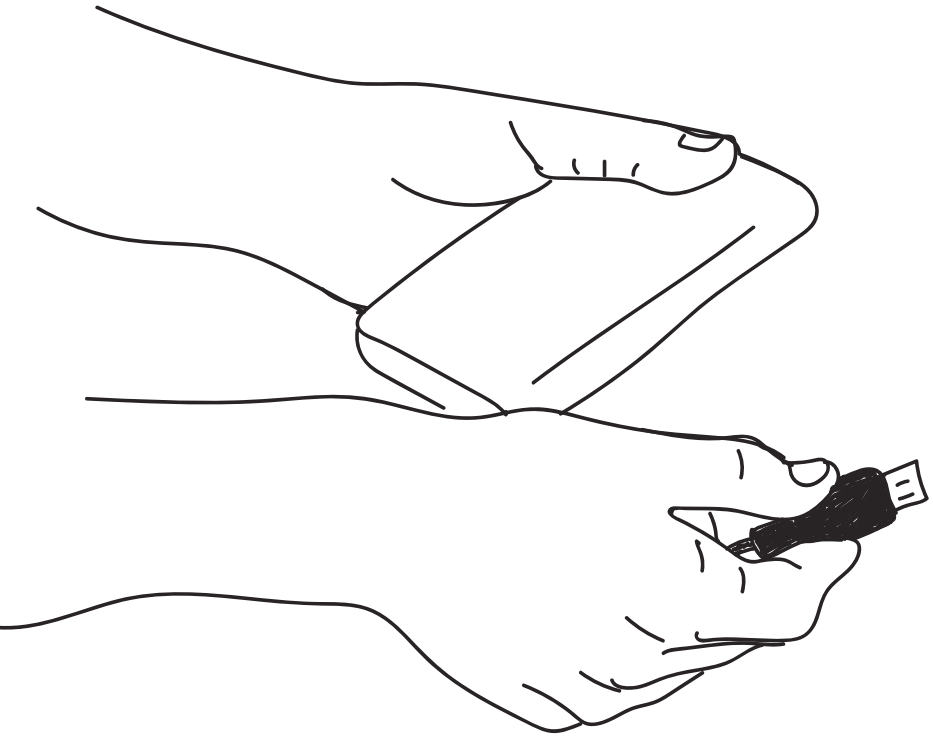
She offers one of her contact centre colleagues £100 to share some card payment details with her and sells this information on for £200, pocketing £100 profit!

Scheming Steve

The Hidden Hacker

Steve is part of your company's IT support team and is regularly sent to fix technical problems in the contact centre. He has come to help clean up Ursula's computer after the unfortunate attack. Steve is a contractor and in his spare time, he enjoys hacking into the systems of large organisations, primarily out of curiosity and because he likes the challenge. While upgrading the security software, he discreetly introduces a Remote Access Trojan, or "RAT" into the machine. This little piece of software allows the device to be accessed remotely. From his home computer, Steve can now hack into the contact centre's network and access customer accounts, along with all the sensitive data he can find in there. Should he choose to do so, he could wreak havoc.





Conniving Carl

The Contract Cleaner

Carl is a hacker who has managed to secure work on a part-time basis for the firm that maintains the building housing your contact centre. He has unrestricted access to every floor and every office. Carl is a skilled computer operator and knows exactly how to go about capturing customer information from the contact centre. While cleaning the office, he slips tiny USB sticks, which contain key logging software and a Wi-Fi transmitter, into several computers. Over the course of the next week, the key loggers capture detailed information of all customer transactions, including payment card numbers. The transmitter sends these to the computer of Carl's associate, who is based elsewhere in the building. Carl returns the following week to remove and collect the USBs, which have gone completely unnoticed.

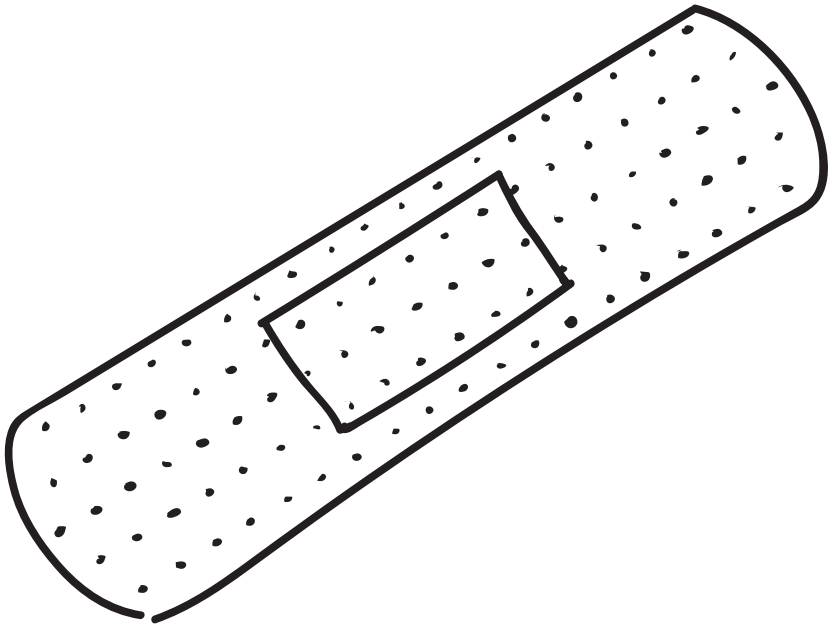
Any one of these five people can bring disaster upon your contact centre. All have the ability to compromise your customer data.

A data breach could mean that you pay thousands of pounds in compensation to your customers. It could mean crippling fines. Above all, however, it could lead to a ruined reputation which undermines your brand and destroys your organisation.

Don’t Compromise Data Security with a Quick Fix

At the heart of the problem is the security of your customer data. If you hold sensitive customer information in your contact centre, you can never be 100 per cent sure that it’s safe. Our recent global survey of over 500 contact centre workers found that 72 per cent of agents who collect payment card data over the phone are still required to ask customers to read card numbers out loud, which raises the danger levels to red. What’s more, some of the measures that are supposed to help protect sensitive data are making matters worse by lulling contact centre managers into a false sense of security.

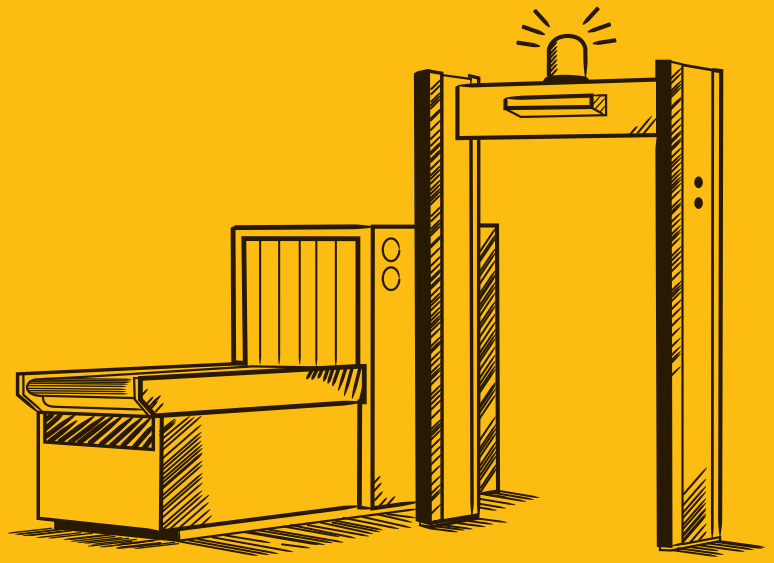
Fortunately, there are a number of ways to strengthen data security and protect sensitive customer information.



Solution 1

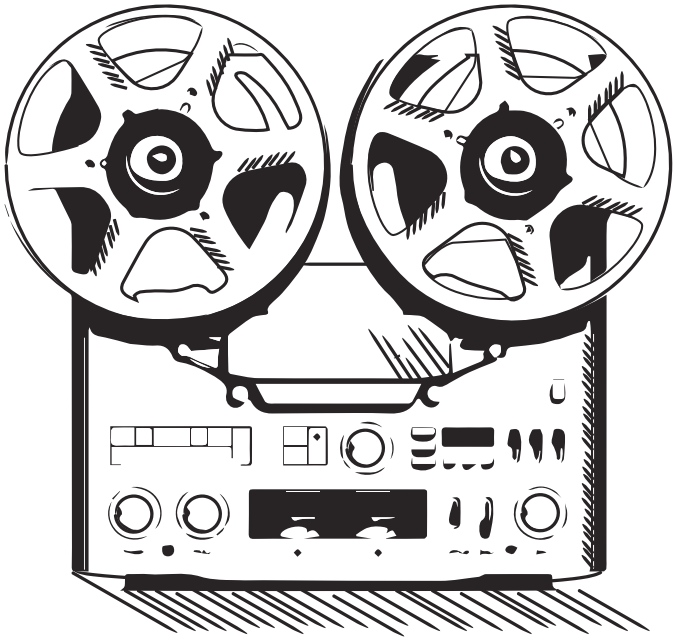
Make your contact centre an ultra-high security zone

Some contact centres take away pens, bags and phones and ask agents to pass through security scanners. This prevents agents from secretly noting down or passing on any payment card details or other sensitive data that they hear.



BUT

It makes working-life miserable, resulting in unhappy agents, high staff turnover and a complete evaporation of trust. And what about your home workers? It is nearly impossible to ensure they are abiding by your security policies – no matter how strict.



Solution 2
Pause and Resume

Capturing sensitive information on a call recording system contravenes the PCI DSS. Some companies avoid doing this by pausing the recording when the customer reads out their payment card details.

BUT

The recording may be paused at the wrong time – whether accidentally or on purpose. What's more, your agent can still hear the card details, and the data touches your desktop, CRM and other IT systems keeping them in scope for PCI DSS compliance.

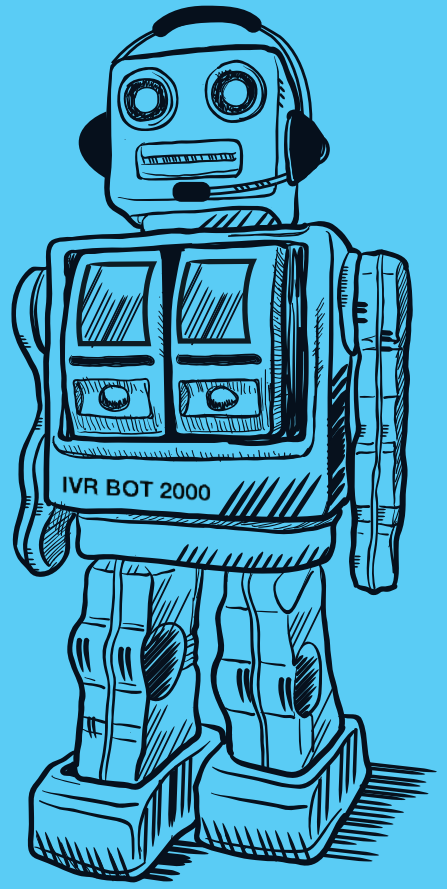
Solution 3

Let a machine take the details

It's possible to pass customers over to an automated Interactive Voice Response (IVR) system, so that the agent doesn't hear any of the details as they are read out loud.

BUT

Customers are only human. They make mistakes and mis-type numbers; and with only a machine to talk to, they often give up and put the phone down. You lose the sale, and you may also lose the customer.

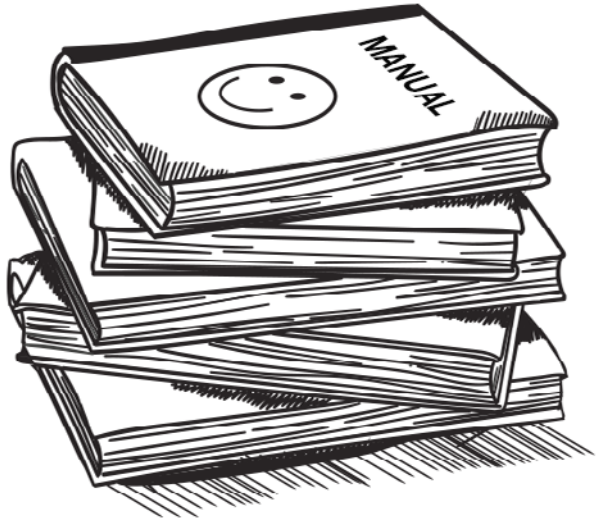


So, What's the Answer?

People are fallible, and we'll never be able to predict and prevent every potential breach. There are, however, a number of steps you can take to reduce risk and keep customer data safe.

1 Properly train (and vet) employees

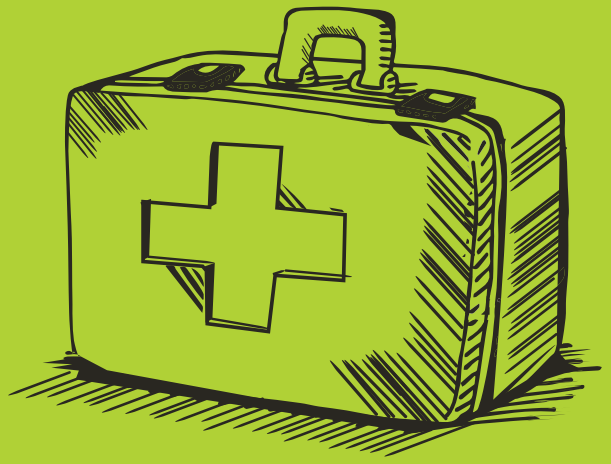
Hiring "good people" is not enough. Train your team properly, treat them well and conduct thorough background checks, even for temporary employees.



2

Implement an incident management policy

Prepare for a worst-case scenario and have a documented Incident Response Plan (IRP) that is tested at least annually.



3

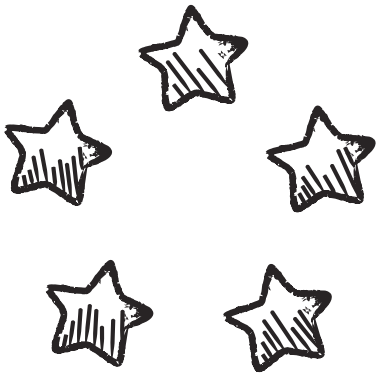
If you must handle sensitive data, use tokenisation

Tokenisation replaces data with a meaningless equivalent while it passes through your hands. Even if a breach is successful, the available data will be of zero value to the cybercriminal.

4

Enforce the principle of Least Privilege – don't give people more than they need

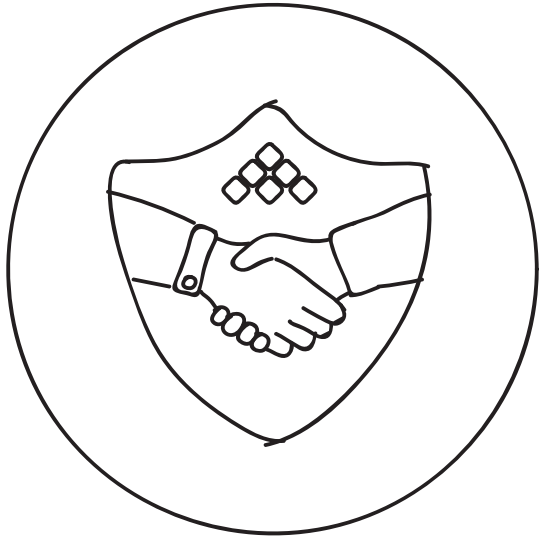
The principle of Least Privilege gives employees the minimum level of access necessary for them to do their job. So, if an agent doesn't need to view customer credit card data when a phone transaction isn't taking place, they shouldn't have access to it at that time.



5

Remove customer data from your contact centre

When sensitive data is exposed to agents and handled and stored in your IT systems, it's just waiting to be compromised. Your objective should be to keep as little of it as possible in your contact centre environment. With **Semafone**, customer data goes directly to the payment provider. Your customers type in the numbers themselves and your agents can't see or hear anything – dual-tone multi-frequency (DTMF) masking technology conceals the sounds they make. And what's more, your agents are able to stay on the line and talk with the caller throughout the call, helping them to complete the payment process.



The Bottom Line

Set your agents free to do their jobs without fear or threat, ensure customer trust and safeguard your company's reputation by investing in technology that de-scopes your contact centre completely.

Semafone is your contact centre data security and compliance expert. We work closely with enterprises around the world to remove sensitive data from IT and business networks – protecting your customers and your company's reputation from fraudsters like those profiled in this guide. Our award-winning, patented data capture method allows contact centre agents to securely capture personal information including payment card data, bank account details and social security numbers over the phone using dual-tone multi-frequency (DTMF) masking technology. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their numbers into their phone keypad, ensuring a positive customer experience. In addition to deterring fraud, we help simplify compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS) so you can focus on business as usual.

To learn more about the risks associated with insider and outsider fraud, download our accompanying research report, **The State of Data Security in Contact Centres**. Based on our survey of more than 500 global agents, this report aims to create a greater sense of urgency among the contact centre community for securing their data now... because, why wait to be breached?

0845 543 0822

info@semafone.com

www.semafone.com

@semafone

Google+

LinkedIn

Pannell House, Park Street, Guildford, Surrey, GU1 4HN

semafone®

securing data · protecting reputations