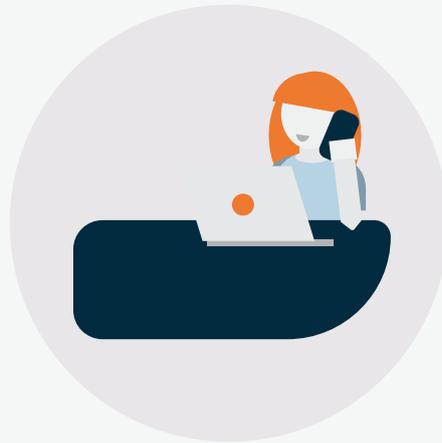
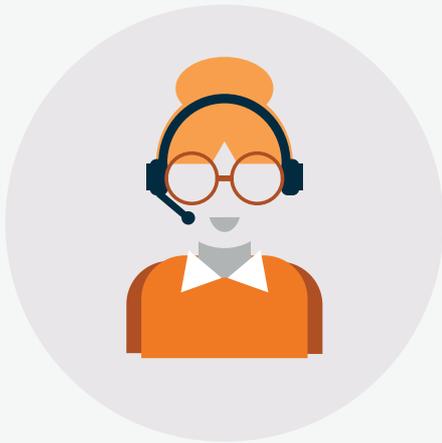


Card Payments by Phone - PCI DSS Compliance

October 2018



The approach

Today, any company that stores, processes or transmits customer data and cardholder information must comply with GDPR and the Payment Card Industry Data Security Standard (PCI DSS). If you're taking card payments over the phone... your business could face hefty fines. But compliance doesn't need be expensive and time consuming. With the right solution, your agents will be able to securely and efficiently deal with each transaction, so that you ultimately take more payments without needing to change your Payment Service Provider.

We offer a PCI DSS v3.2 compliant service as either a standalone solution that works with your existing set-up, or as part of a multi-channel contact centre solution. Working with our trusted partner, Real Credit – a Level 1 compliant provider of secure card payment services – we can ensure sensitive credit and debit card information is no longer visible within your organisation, passing responsibility for compliance to Real Credit, so you can get back to focussing on your business.



How it works...

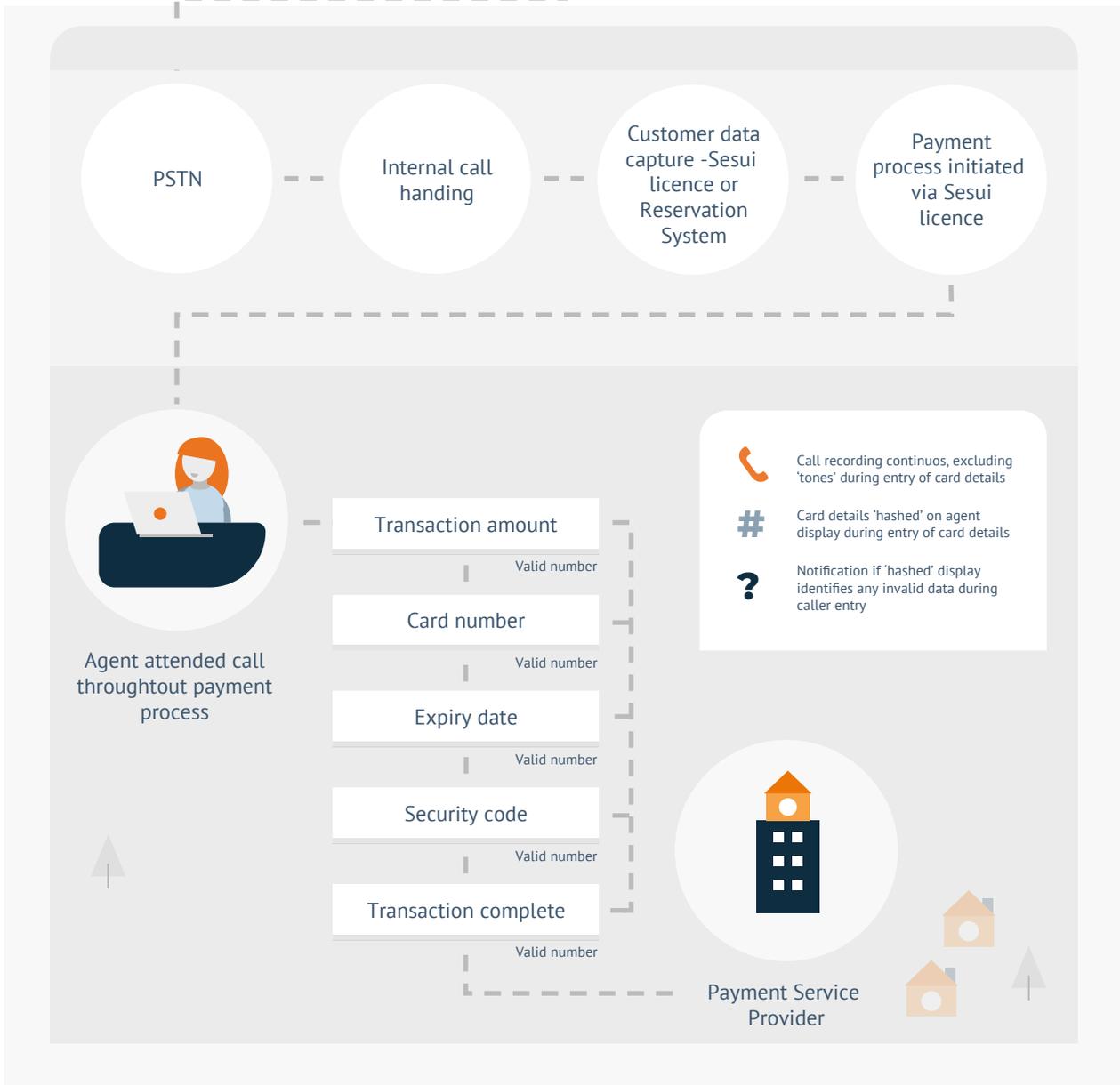
If a customer call results in a credit or debit card transaction, the caller will use their keypad to enter their long card number, expiry date and security code on the back of their card. This results in a Dual Tone Multi Frequency (DTMF) "tone" being sent to our Sesui system, which we then block from reaching your agent. Your agent, who stays connected to your caller throughout the process, will receive screen notifications so they can follow the caller's progress, but never hears any of tones or sees any card data. It means if the customer's data fails to pass basic check - such as a wrongly entered expiry date - your agent can prompt them to try again.

Once all of the data has been entered, the transaction is forwarded to our payment provider, Real Credit, for processing while your agent and caller stay connected.

Real Credit then provides a unique "token" which is used to identify the card details when processing any subsequent payment requests. This "token" can then be entered into the CRM database, in lieu of card details, ensuring sensitive information is ONLY stored on Real Credit's highly secure PCI-DSS compliant system.

Because so many organisations depend on calls being recorded and stored for playback purposes or for compliance, our PCI DSS service ensures you still get a complete recording of the discussion, but without recording the data entry part of the call.

Sesui Card Payments



So if you need a solution that...

- Works with your existing Payment Service Provider such as Sage Pay and Verifone
- Stores call recordings securely in the cloud, with easy to use search functions
- Integrates with one of our contact centre solutions, so that call activity is controlled and completed from a single screen
- Ensures your agent stays connected throughout the call, without hearing any of the tones, seeing any card details, or needing to hand-off the call or “pause and resume”

Then call us on 03445 600 600.

We're Sesui. We make vital connections.

Sesui
cloud communications



@Sesui_ltd



@Sesui-ltd



03445 600 600

