Why Gala Tent created Gala Technology

This case study demonstrates how, over a 4 year period, a small innovative UK manufacturing business eliminated chargebacks from payments taken in their telephony channel and built an award winning, patented technology that can now benefit all stakeholders in the card payments ecosystem.

The case study follows Gala Tent's story, illustrating how they grappled with a high volume of chargebacks, the initial "fraud screening" efforts they deployed to reduce the number of chargebacks and loss of product the customer frustration because of the elongated identity verification processes and Gala Tent's frustration at having to turn away good business. The study describes the technology Gala Tent developed in-house to improve the customer experience and reduce overall operating costs, how Gala Tent has set about making the technology available so that other merchants can benefit from reducing chargebacks and overall risk when handling telephony transactions in the more fraud prone Card Not Present [CNP] payment channels, which is arguably one the biggest challenges facing the card based payments today.

Introduction and context

Gala Tent opened for business in 1999, in response to demand for event marquees for the millennium celebrations. By 2012 the company had established itself as the leading European supplier of marquees and gazebos to the events industry, with manufacturing facilities in China and distribution throughout Europe. Turnover had grown to £5m ($6m) per annum with circa 10,000 transactions annually via ten full time sales agents processing primarily telephone orders via virtual terminals, with call recording in the background.
In spring 2012 the company found itself receiving a large number of chargebacks from fraudulent CNP MOTO transactions, presumably as a result of being targeted by criminals. Offering national next day delivery on high value items, the company was an easy target for CNP card payment fraud and began to realise how exposed they were to fraud and its associated costs in terms of lost stock, chargebacks and increased card transaction charges.

The problem

The catalyst was a £9,000 order from an Events Agency in London, who requested that the order be delivered to a remote location in the Midlands. The order was taken, the card number was also taken and key entered into a virtual terminal. The card payment was verified to a 3rd party delivery address and the order was despatched. A chargeback was received once the genuine card holder received an unexpected bill. The PSP defended its position referring Gala to their terms and conditions. Gala challenged on the basis that the card payment was authorised, but the response received indicated that it was an un-secured telephony payment and included a £20 administration charge.

Without a way to verify customers' identities over the telephone, Gala Tent had to take onboard the published advice, to only deliver to a registered cardholder address. In an attempt to protect themselves Gala Tent established a 'Fraud Prevention Team' to physically review the number of customer identification checks the Fraud Prevention Team now felt was needed. This involved diverting existing resources, hiring new staff and putting additional processes in place to authenticate customer ID and validate 3rd party delivery addresses and the customer's access to that address. This included using Google Earth to establish location and Facebook to validate identity, asking for personal ID to be faxed & utility bills for the 3rd party addresses. The list went on, all of which created a bad buying experience for the customer. These additional process steps added significantly to the cost of the sale because of staff time needed to support the number of interactions required with the customer to complete the order. By mid-summer, the costs in lost stock, lost sales (where good sales were lost) plus additional staff costs and the inability to seamlessly deliver to a 3rd party address, meant that the overall cost of MOTO payments was circa £50,000 per month ($60,000) pcm, an unsustainable situation, even for peak trading levels.

Gala Tent's situation was not uncommon. By 2012 figures published by the Financial Fraud Action Group (FFA UK) indicated CNP fraud had grown, as Chip & Pin was rolled out. CNP figures have shown over recent years that

fraud was not going away. It simply diverted to more vulnerable payment channels. The banks reflected this in their terms and conditions:

- Sage Pay's fraud prevention guide indicates that it is important to note that Authorisation does not guarantee against chargeback***.*** *"Because the card and cardholder are not present, you are unable to physically check the card or the identity of the cardholder. You therefore need to be particularly careful about CNP transactions, because it is much easier for the fraudster to disguise their true identity...* ***You are responsible for ensuring that CNP transactions are not fraudulent. If a transaction is fraudulent, you will be liable for the loss. You need to ensure that you have procedures in place to protect your business against fraud."***
- Other PSPs offer similar advice, an organisation processing circa 42% of UK payments states: *"Whilst the majority of transactions will be genuine this type of transaction (CNP) is appealing to fraudsters whose main interest is obtaining goods that can be easily re-sold for cash. You should take extra care and consider the risks before you process CNP transactions because you will be financially liable if a transaction is confirmed as invalid or fraudulent. Orders where the delivery address is different from the billing address may be legitimate (for example, when sending flowers or a birthday present) but we always recommend, where possible, you deliver to the cardholder's billing address."* The text continues *"For mail and telephone order transactions - Although there is no guarantee of payment, delivery to the cardholder's billing address provides comfort that the genuine cardholder is receiving the goods. There is an increased risk to your business if the transaction is later confirmed as fraud as you may be held financially liable. For eCommerce transactions – if you have implemented MasterCard Secure Code and Verified by Visa (known as cardholder authentication) provided that the process is carried out correctly, your business will be protected against fraud related chargebacks."*

The solution – leverage 3D Secure

The solution had to be to either automate the 'fraud prevention department' process in some way or develop an application that negated the need to frustrate the sales process that was making a telephony purchase a negative experience for the customer. The answer was to leverage the card schemes' existing processes in the e-commerce channel to protect against fraud related chargebacks, by using 3D Secure, in the telephony payment, as a verification method, in the same way as it is used in the e-commerce environment, thereby shifting the risk of fraud away from Gala Tent and back to the issuer.

The solution developed ensured that Gala Tent's staff could remain in constant voice contact with the customer to make certain that the order process was concluded and to secure up-sells, even to 3rd party delivery addresses. Over the next 12 months (2012/13) Gala Tent developed what they called internally their Secure Order Transfer solution that met their objectives: using 3DSecure to validate the customers' identity and secure the transaction, whilst providing a fully supported and seamless customer experience.

Transforming the un-secured telephony payment to a secure 3D secure e-commerce payment.

The outcome – zero Chargebacks & reduced operating costs and stock loss

After trials and roll out across the sales and service team, the results were immediate:

- Customer details were no longer needed so the Fraud Prevention Team's staff was redeployed and the organisation began to process more orders successfully without the burden of chargebacks
- In operational terms, deployment of the solution reduced the number of times Gala Tent had to interact with the customer to secure the sale consequently the average time on the phone was reduced from over 10 minutes per call to less than 2½ minutes
- The conversion rate from call to order doubled from circa 40% to 80% helping drive overall sales from £5M to £10M since deployment, supporting proportional growth in operating margins
- In terms of e-commerce vs telephone split, despite significant investment over the last 36 months in their ecommerce engine, telephone orders now account for circa 82% of Gala's revenue. It appears that customers feel more re-assured purchasing high value products by telephone

From a payments compliance standpoint, deploying the Sales Order Transfer solution meant that payment card data was no longer entering Gala Tents' environment. This meant that instead of having to complete a SAQ D,

they were in a position to complete SAQ A to meet their PCI DSS compliance obligations, again saving time, effort and costs to the business

Early success acknowledged and rewarded

After early stage deployment in 2013, Gala Tent was encouraged by their regional business community to enter their solution into the 'Security Innovation of the Year' section and were awarded 'The National UKIT Awards'. Attending the Awards Dinner in 2014, and knowing their entry had been shortlisted with 10 others including British Telecom, it was to their utter surprise that Gala Tent's Secure Order Transfer solution was voted by the judges as the winner. This prompted Gala Tent Limited to establish Gala Technology Limited.

Sharing the benefits with the global secure payments community and the merchants they support

Gala Technology Limited was established in 2015 to drive the commercialisation of the 'sales order transfer process' renamed as SOTpay. In 2016, Gala Technology engaged with contact centre payments and payments compliance specialists Compliance3 to help set the bar in terms of documentation and process requirements to support scalability and growth. The first step was an introduction to world leading risk management business, Coalfire Inc, to make recommendations on infrastructure partners (Armor), validate payment card flows and documentation and sign off the product in line with SAQ D SP.

SOTpay is now available as an affordable transaction based secure payments solution, that is robust, scalable and can be effectively deployed as part of a merchants telephone environment fraud management and scope reduction strategy. From a PCI DSS perspective, unlike other solutions previously offered for this channel, at a cost-effective price that can directly impact on the reduction of fraud, eliminating merchant costs for fraud related chargebacks. As part of a PCI scope reduction programme, SOTpay can reduce the time, cost and effort in completing annual PCI compliance assessments, which means no non-compliance fees and potentially lower transaction charges.

Changing the early drafting of the current PCI SSC guidelines on protecting telephone-based payment card data

On the back of leading the project that enabled a large European multi-channel retailer become the first merchant globally not to have a card data environment in 2013, John Greenwood started his journey to persuade the PCI Security Standards Council (PCI SSC) to update their guidance on protecting telephone-based payment card data, first published in 2011. That guidance focused on securing the recording of payment card data but missed the opportunity to fully acknowledge the contact centre as a central part of entities customer communication strategy. The main point being, that as the internet became more secure, the telephone channel would become the 'soft underbelly' of the secure payments ecosystem.

By 2015, with DTMF based technology vendors becoming more established, they formed a strong lobby to dominate the guidance update, and for obvious reasons. However, after seeing a demonstration of SOTPay and the ability to operate across voice and non-voice customer communication channels (such as web-chat and social media), John was able to extend his initial classification of 'scope reduction technologies' in his early drafts to the PCI SSC.

On the 27th of November 2018 the Payment Card Industry Standards Security Council published their new 70 page PCI information supplement Protecting Telephone-Based Payment Card Data replacing the 12 page information supplement of the same title published in March 2011. The relevance of this new guidance is only fully understood when considered in the context of the PSD2 Regulation reducing ecommerce fraud and that displaced fraudulent activity being focused on the more vulnerable MOTO channel.